Giegerich & Partner

gpg4o

Manual
Version 3.5

Table of Contents

1 General **4**

2 System Requirements **5**

3 Functional Range **6**
3.1 Versions Functional Range Comparison 6
3.2 After the expiration of the product maintenance 7
3.2.1 Trial version 7
3.2.2 Home & Student Version and Full Version 7
3.3 PGP/MIME 7

4 Installation **8**
4.1 Software 8
4.2 Installing gpg4o 8
4.3 Configuring gpg4o 12
4.3.1 Information about gpg4o 17

5 Licence-Files **19**
5.1 Generating and Importing License-Files 19
5.2 Period of Validity of the License 22
5.3 Period of Validity of the Product Maintenance/Support 22
5.4 Extension of the Product Maintenance 22

6 Utilizing gpg4o **24**
6.1 Sending Public Keys 24
6.2 Importing Public Keys 25
6.3 Sending Encrypted and/or Signed Messages 26
6.3.1 Manual assignment of keys 28
6.3.2 Virtual Accounts 30
6.4 Receiving of Encrypted and/or Signed Messages 30
6.5 Sending and Receiving Encrypted Attachments 32
6.6 Reply/Forwarding of emails in Outlook 2013 onwards 32
6.7 Printing Encrypted Messages 33
6.8 Permanent Decrypted Saving 33
6.9 Hide Send Options 34

7 Key Management **35**
7.1 General Information Regarding Keys 35
7.2 Overview 35
7.3 Modifying View 36
7.4 Filtering Keys 37
7.5 Generating New Keys 37
7.6 Deleting Keys 38
7.7 Enabling/Disabling Keys 38
7.8 Exporting Keys 39

7.9 Importing Keys . . . 39
7.10 Key Details . . . 41
7.10.1 Summary . . . 42
7.10.2 Private Key . . . 43
7.10.3 Identities/Signing . . . 44
7.10.4 Public Key . . . 45
7.10.5 Define Owner Trust . . . 46
7.11 Utilization of Keyservers . . . 47
7.12 Generating Revocation Certificate . . . 49
7.13 Applying Revocation Certificate . . . 50

8 Sending Rules 52
8.1 Management of Sending Rules . . . 52
8.2 Rule Evaluation . . . 53

9 Settings 56
9.1 View . . . 56
9.1.1 Language . . . 56
9.1.2 Encryption Status . . . 56
9.1.3 Send Options . . . 57
9.1.4 Messages . . . 57
9.2 GnuPG . . . 57
9.2.1 Path to gpg.exe/gpg2.exe . . . 58
9.2.2 GnuPG Version Checking . . . 58
9.2.3 GnuPG Directory . . . 59
9.2.4 GnuPG Agent . . . 59
9.2.5 Buffering of the Passphrase . . . 59
9.3 Account Management . . . 59
9.4 Settings for Sending and Receiving . . . 61
9.4.1 Domain Based Key Search . . . 61
9.4.2 Attachment Send Options . . . 62
9.4.3 Public Folder . . . 62
9.5 Update . . . 62
9.6 Keyserver . . . 64
9.6.1 Keyserver . . . 65
9.6.2 Autoimport . . . 65
9.7 Backup . . . 65
9.8 System Information . . . 67
9.9 Extended Settings . . . 67
9.9.1 Always treat all keys as valid . . . 67
9.9.2 Insert GnuPG and gpg4o information in outgoing emails . . . 68
9.9.3 Advanced signature check activation . . . 69

10 Miscellaneous 70
10.1 What Is to Be Done in Case of Errors? . . . 70
10.2 gpg4o does not Start . . . 70
10.2.1 Disabled Application Add-ins . . . 71

10.2.2 COM-Add-Ins 71
10.2.3 Microsoft Outlook 2013® and Outlook 2016® 71

11 Help Center **73**
11.1 Sending Log-Files 73
11.2 Contents of Log-Files 74

12 Uninstalling **75**
12.1 Delete personal Data 75
12.1.1 GnuPG Directory 75
12.1.2 gpg4o User Directory 75
12.1.3 Microsoft Outlook® Configuration Directory 75
12.2 Uninstalling under Windows Vista, 7, 8 or 10 75
12.3 Uninstalling GnuPG 75

13 Contact & Information **77**

1 General

gpg4o – GPG for Outlook

gpg4o was developed as an add-in for Microsoft Outlook 2010® , Microsoft Outlook 2013® and Microsoft Outlook 2016® and is supported by the 32- as well as by the 64-bit version.

gpg4o assures a safe electronic communication by encrypting and decrypting emails and their file attachments. Of course, signing and verifying is also possible.

The integrated key management by **gpg4o** provides the simple and uncomplicated handling of public keys.

The validity of external keys is verified by means of the Web of Trust function. For this purpose information of known key owners is used.

2 System Requirements

In order to be able to utilize **gpg4o**, your system must fulfill at least the following requirements:

Operating System:

- Microsoft Windows Vista from SP1 onwards
- Microsoft Windows 7
- Microsoft Windows 8.x
- Microsoft Windows 10

Email program:

- Microsoft Outlook 2010® 32- or 64-bit version
- Microsoft Outlook 2013® 32- or 64-bit version
- Microsoft Outlook 2016® 32- or 64-bit version

GnuPG

- GnuPG 1.4, Version 1.4.19 onwards
- GnuPG 2.0, Version 2.0.29 onwards
- GnuPG 2.1, currently **not** supported

3 Functional Range

3.1 Versions Functional Range Comparison

Function	Test Version	Home & Student Version	Full version
Encrypt, decrypt, sign emails	✓	✓	✓
Simultaneously usable email accounts	1	optional	optional
Private/commercial use	✓ / ✓	✓ / ✗	✓ / ✓
HTML emails	✓	✓	✓
„Plain-Text“ emails	✓	✓	✓
Display of PGP/MIME emails	✓	✓	✓
Individual sending rules	✓	✗	✓
Decrypted saving of emails	✓	✗	✓
Period support	45 days [1]	1 year [2]	1 year [2]
Period update	45 days [1]	1 year [2]	1 year [2]
Period usability	45 days [1]	unlimited	unlimited
Supported mail servers			
Microsoft Exchange	✓	✗	✓
POP3	✓	✓	✓
IMAP	✓	✓	✓
Outlook.com	✓	✓	✓
Hotmail.com	✓	✓	✓
Supported software			
Outlook versions until 2007	✗	✗	✗
Outlook 2010, 32/64 bit	✓	✓	✓
Outlook 2013, 32/64 bit	✓	✓	✓
Outlook 2016, 32/64 Bit	✓	✓	✓
Windows Vista from SP1 onwards, 32 bit	✓	✓	✓
Windows 7, 32/64 Bit	✓	✓	✓
Windows 8.x, 32/64 Bit	✓	✓	✓
Windows 10, 32/64 Bit	✓	✓	✓
Compatible with DATEV installations	✓	✓	✓

[1] Extension of the test period is possible on request

[2] Depending on the duration of product maintenance (1 year after purchase, afterwards extensible by purchasing an extension of product maintenance: +1 year, +3 years or +5 years)

3.2 After the expiration of the product maintenance

3.2.1 Trial version

You can only decrypt emails which were received during the test period. Emails can no longer be sent encrypted / signed.

3.2.2 Home & Student Version and Full Version

When the product maintenance has expired **gpg4o** can still be used. That means that you can continue to send encrypted / signed emails and read encrypted / signed emails. It is simply no longer possible for you to install new updates or to make use of the support.

3.3 PGP/MIME

gpg4o can send and receive plain text messages and HTML emails as PGP/Inline. In addition PGP/MIME emails can be received and decrypted. It's also possible to verify PGP/MIME („detached signature“) signed emails.

4 Installation

4.1 Software

The latest download version of **gpg4o** can be found at:

http://www.giepa.de/produkte/gpg4o/downloads/

For the use of **gpg4o GnuPG** is required. You may have **GnuPG 1.4** installed during the first configuration of **gpg4o**.

Information and the source code of **GnuPG** can be found at:

http://www.gnupg.org/

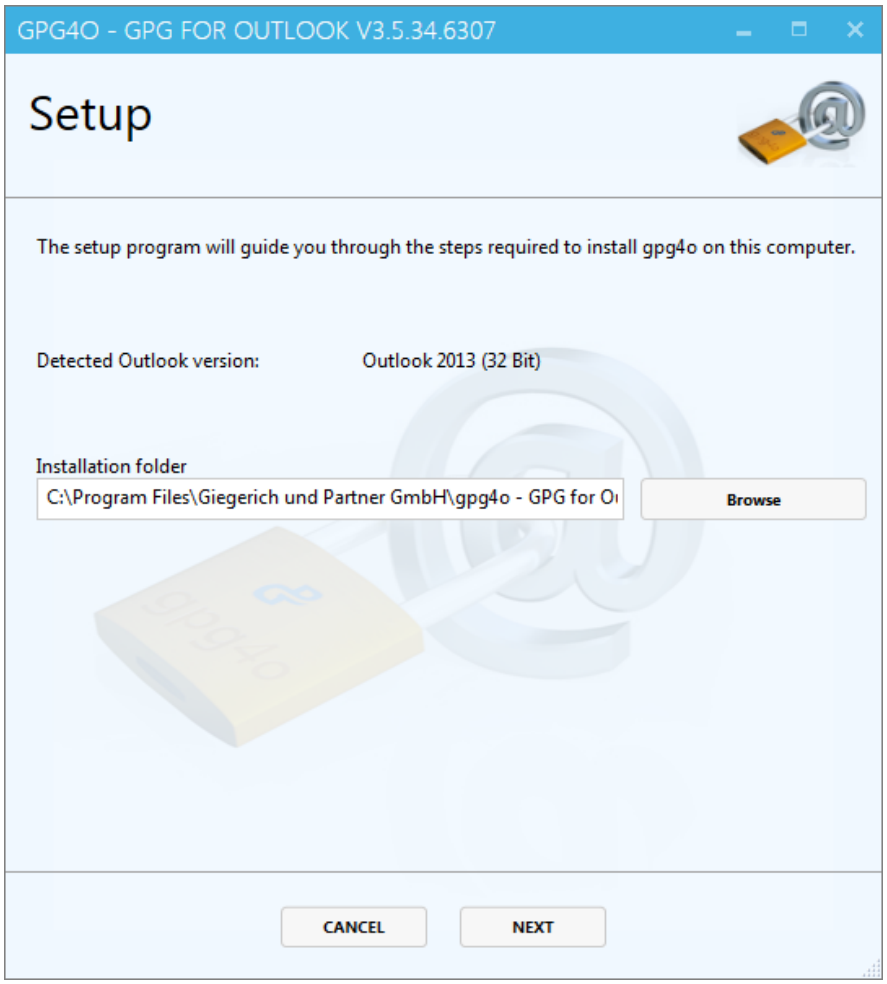
The General Public License (GPL) can be found at:

www.gnu.org/licenses/gpl.html

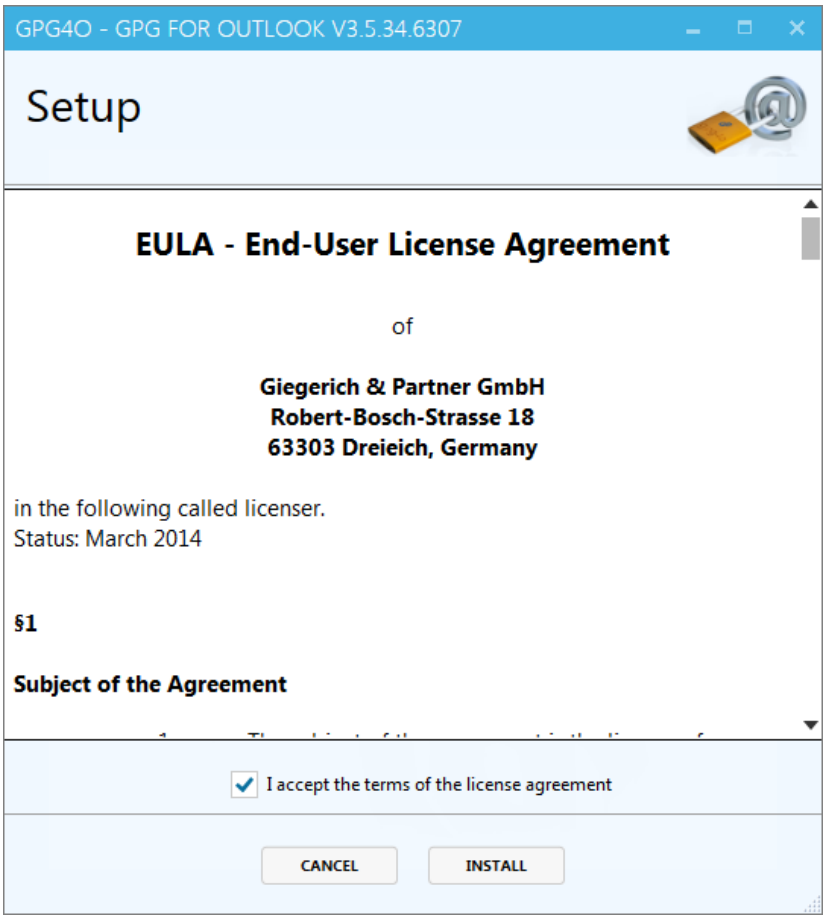
4.2 Installing gpg4o

For the installation you need administrative privileges. Before installing **gpg4o** please close the application Microsoft Outlook® , as otherwise, there might be problems during installation. Having done this, execute the file **„gpg4o_setup.exe“** by double-clicking it.

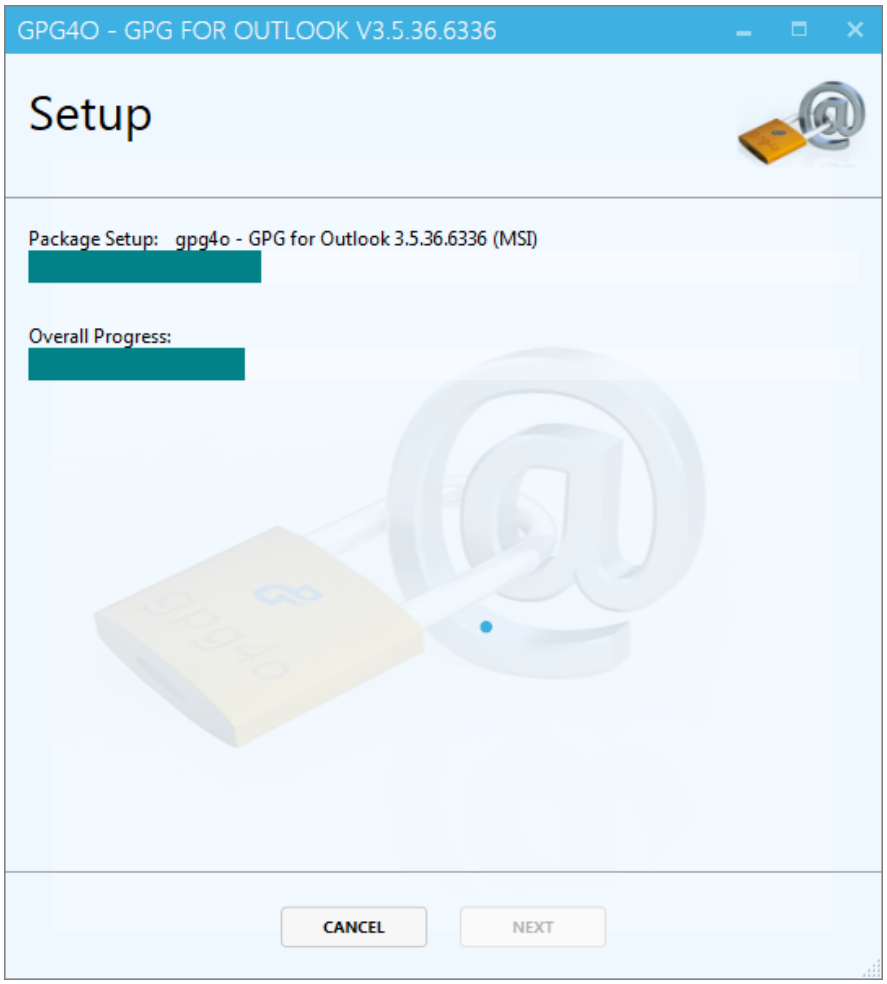
In the following start-dialog you will be asked to set the installation path. Here the default setting is normally the best choice. Confirm the installation path by clicking on **„NEXT“**.



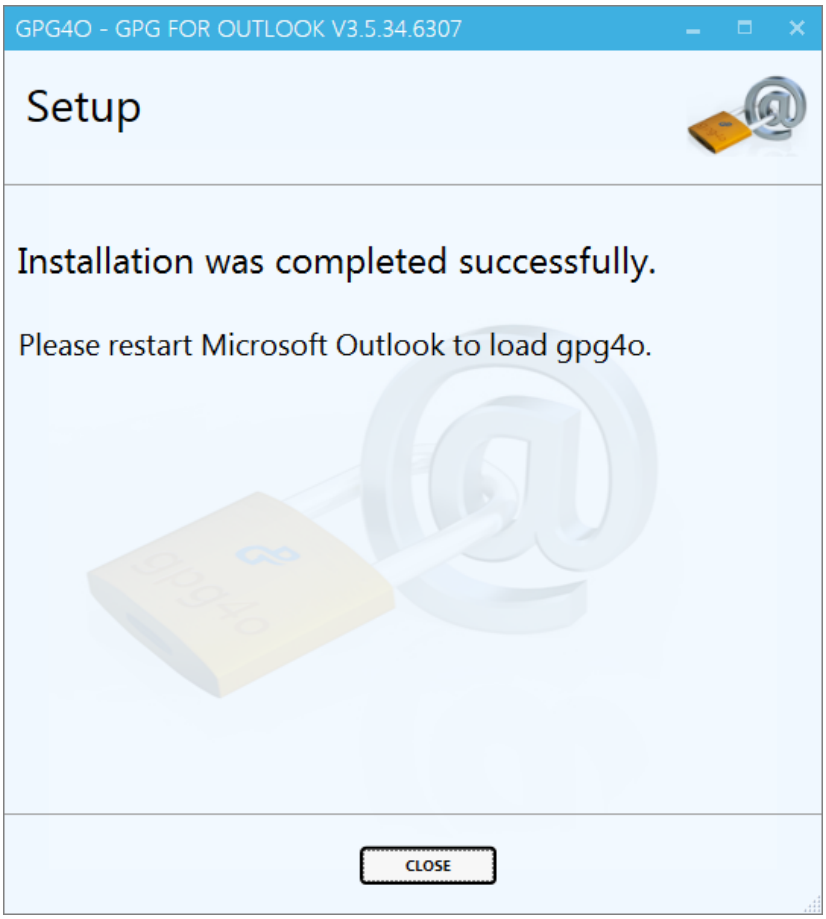
In the following dialog you will see the End-User License Agreement. Once you have decided to accept the License Agreement (precondition for the installation), select the radio-button next to **„I accept the terms of the license agreement“** and click **„INSTALL“** to continue the installation.



The installation will start now. In doing so, the presence of all required components (for example .NET Framework 4) is checked. Missing components will then automatically be installed. As soon as all the necessary components have been installed, the wizard will continue installing **gpg4o**.



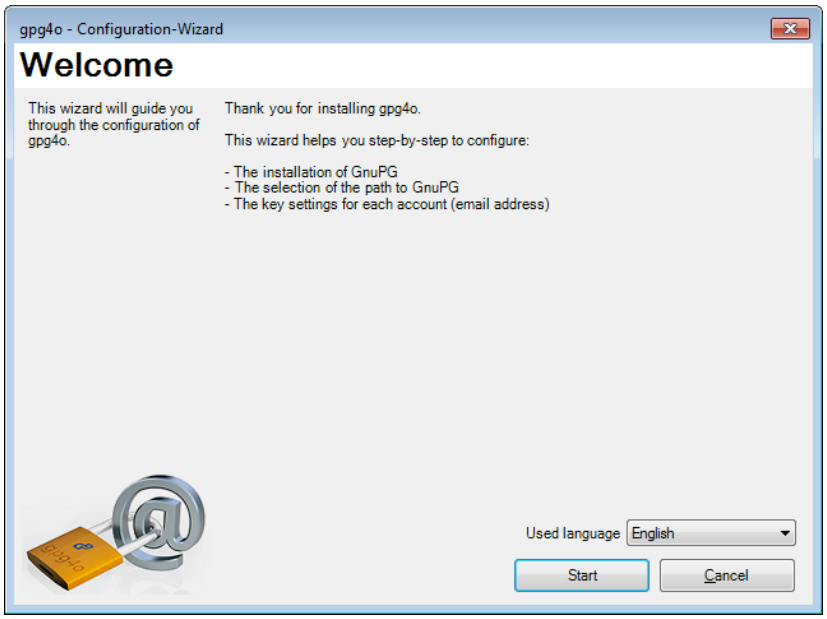
Now the installation of **gpg4o** is completed. You can start the configuration of **gpg4o** by restarting Microsoft Outlook® .



4.3 Configuring gpg4o

Start Microsoft Outlook® now in order to begin the configuration of your new software. The configuration wizard appears which will help you to set up **gpg4o**.

In addition you have the possibility of changing the language of **gpg4o**. Once you have selected your language, click **„Start“** in order to begin the configuration.



On the second page of the configuration wizard the required component **GnuPG** will now be configured.

*View when no valid **GnuPG** installation could be found.*

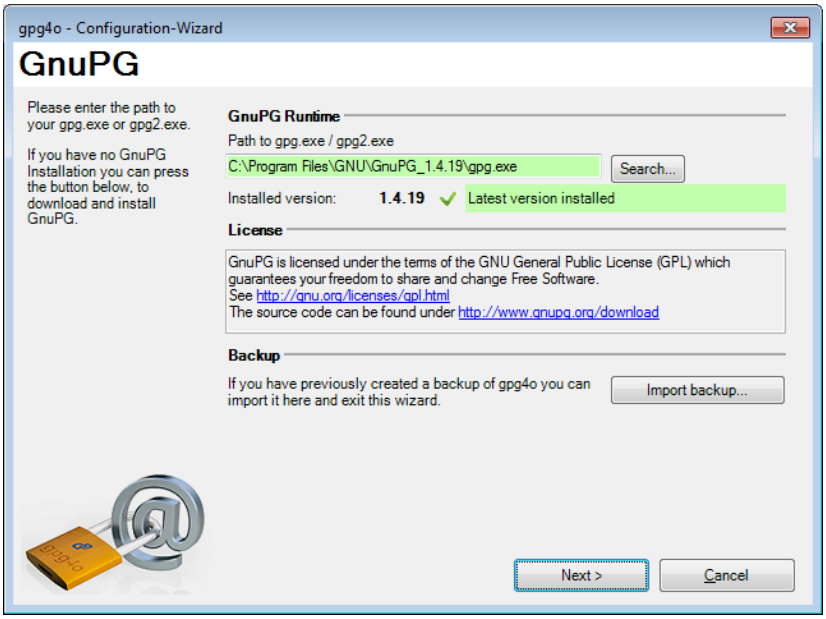
If **GnuPG** is already installed on your computer, the path will automatically be entered and highlighted green. If the installation path of **GnuPG** cannot be found, the selection will be highlighted reddish. In this case click **„Search“**, search on your hard disk for the **GnuPG** installation and select the file **„gpg.exe“** or **„gpg2.exe“** in the **GnuPG** installation folder. The installation path should now be highlighted green.

You can also download **GnuPG** from the Internet and have it installed. For this purpose, click **„Download and install GnuPG“**. A folder selection will appear. Please select a directory

where **GnuPG** shall be installed.

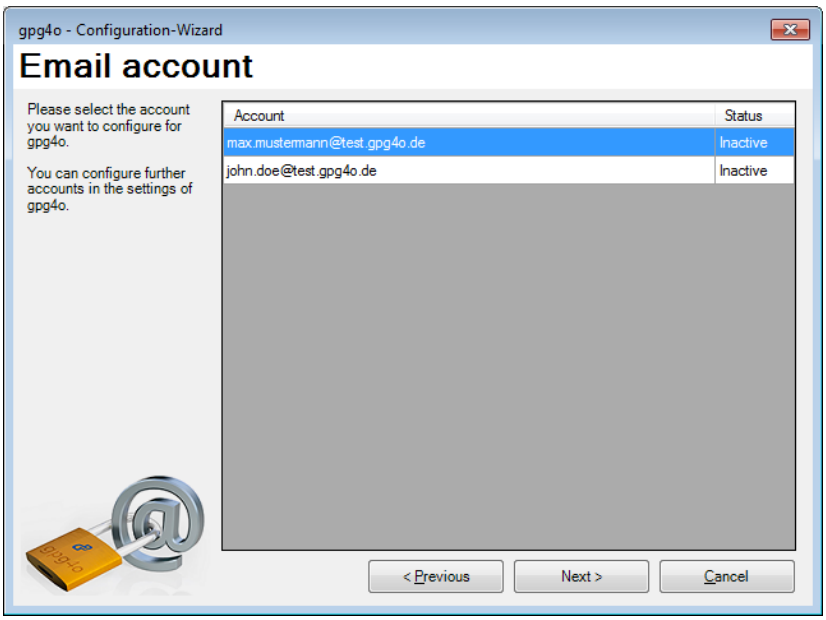
Hint: Please make sure that the directory where **GnuPG** shall be installed is empty.

After a successful installation the path will be automatically applied into the settings and you may continue the configuration.



Alternatively, you can import a backup of **gpg4o** here (see paragraph 9.7).

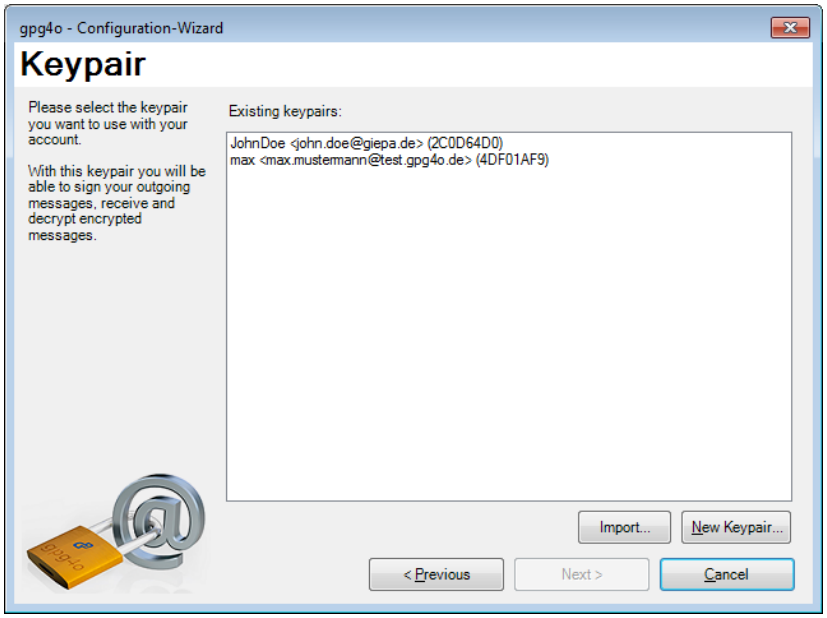
Next you will be asked for which email account you want to install **gpg4o**. This page only appears if you have configured more than one email account in Microsoft Outlook® .



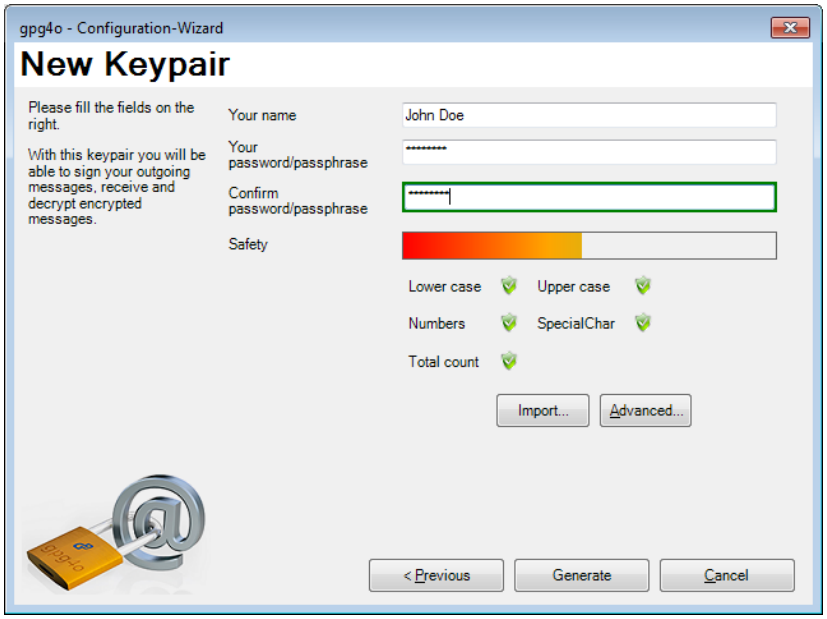
Select the account with which you want to utilize **gpg4o**. Having done this click **„Next >“**.

Hint: Further accounts can be configured subsequently in the settings of **gpg4o**.

If you have already applied **GnuPG** before you can now select an existing keypair with which **gpg4o** shall sign messages.



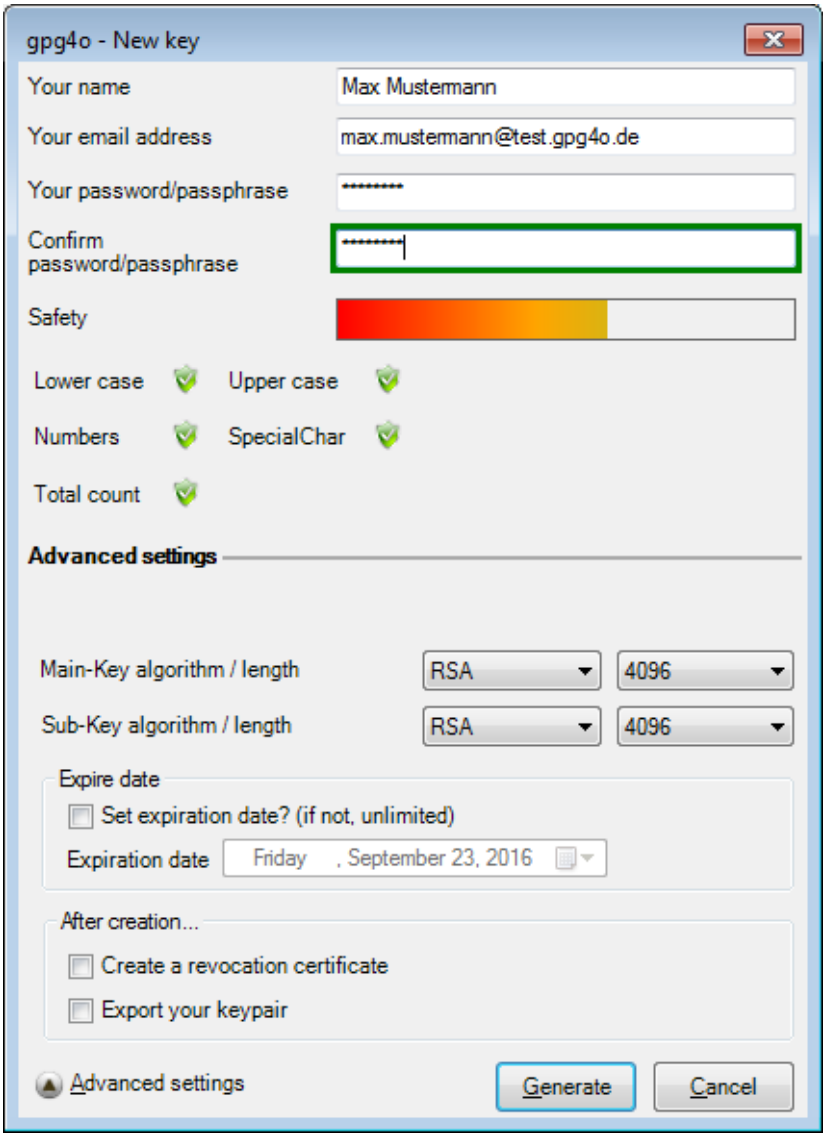
If you do not yet have a keypair or if you want to generate a new keypair the page **„New Keypair“** will directly appear instead.



In order to generate a new keypair enter your name first, as shown in the screenshot above, as well as a passphrase. After having filled all required fields, click **„Generate“** and your new keypair will be generated.

If you want to make further settings for your new keypair you can call an advanced dialog with additional configuration possibilities by clicking **„Advanced...“**.

Alternatively, you have the possibility of importing a keypair which you have already generated in the past. For this purpose, click **„Import...“**.



In the advanced settings you may influence the algorithms and the length of the key. The default setting, however, already offers maximum safety.

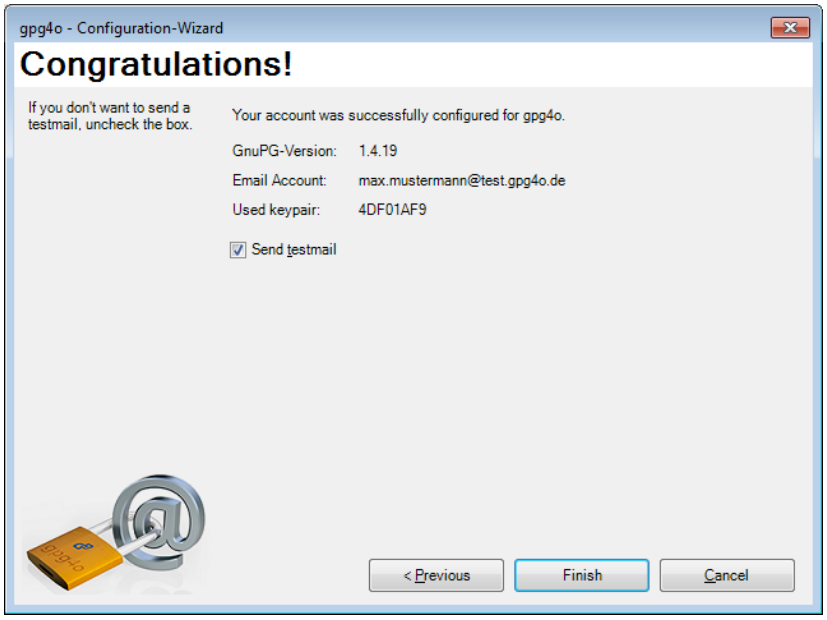
Moreover, you can define an expiration date for the key. After this period the key can no longer be utilized in order to sign or encrypt messages. Decrypting, however, will remain unaffected.

It is also possible to provisionally generate a revocation certificate if your key gets lost. You should keep this certificate safe as it is the only possibility to invalidate your key (see paragraph 7.12).

Last you may also export the keypair. This data backup should be kept very safe. Please

mind that the exported keypair may only be utilized with the passphrase which was entered during generation.

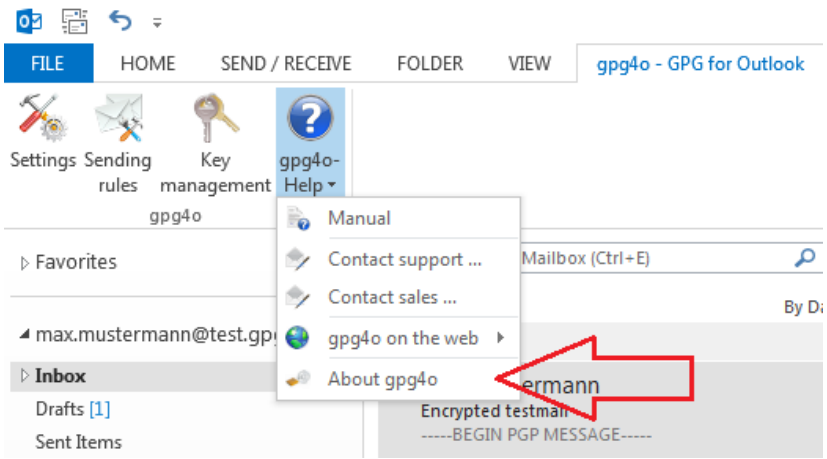
Finally, you will find a brief summary which email account was configured with which keypair as well as the **GnuPG** version you utilize.



If you leave the checkmark with **„Send testmail“** an encrypted test message will be sent to you automatically with which you can check the configuration of **gpg4o** as soon as you have clicked **„Finish“**.

After a successful installation you will see a new tab named **„gpg4o - GPG for Outlook“**, if you look at the menu ribbon in Microsoft Outlook® . Here, you will find the key management, sending rules and the possibility of modifying your settings.

4.3.1 Information about gpg4o



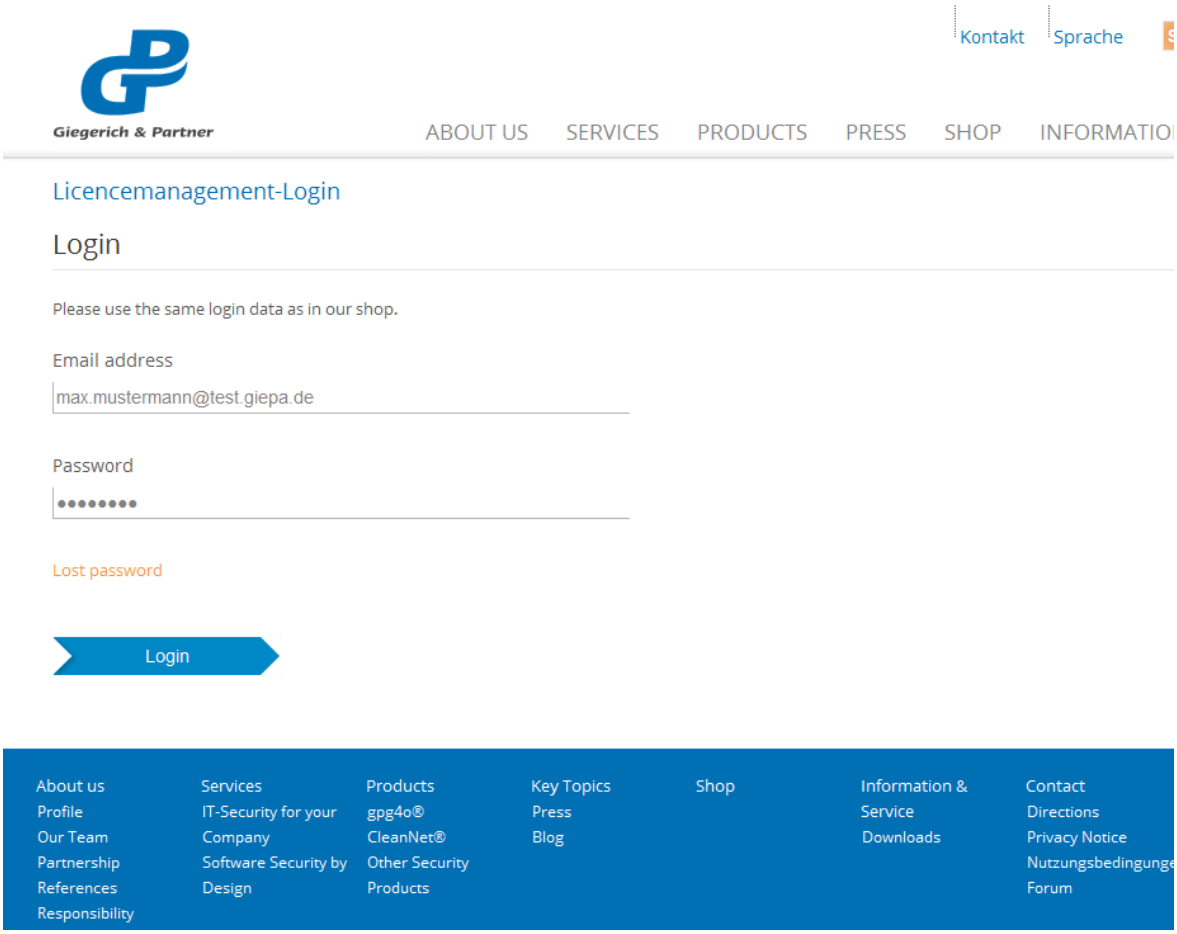
For more information to **gpg4o**, please click on **„gpg4o-Help“** and **„About gpg4o“**. In the following window, you can see information to your license and information to the currently

installed version.

5 Licence-Files

5.1 Generating and Importing License-Files

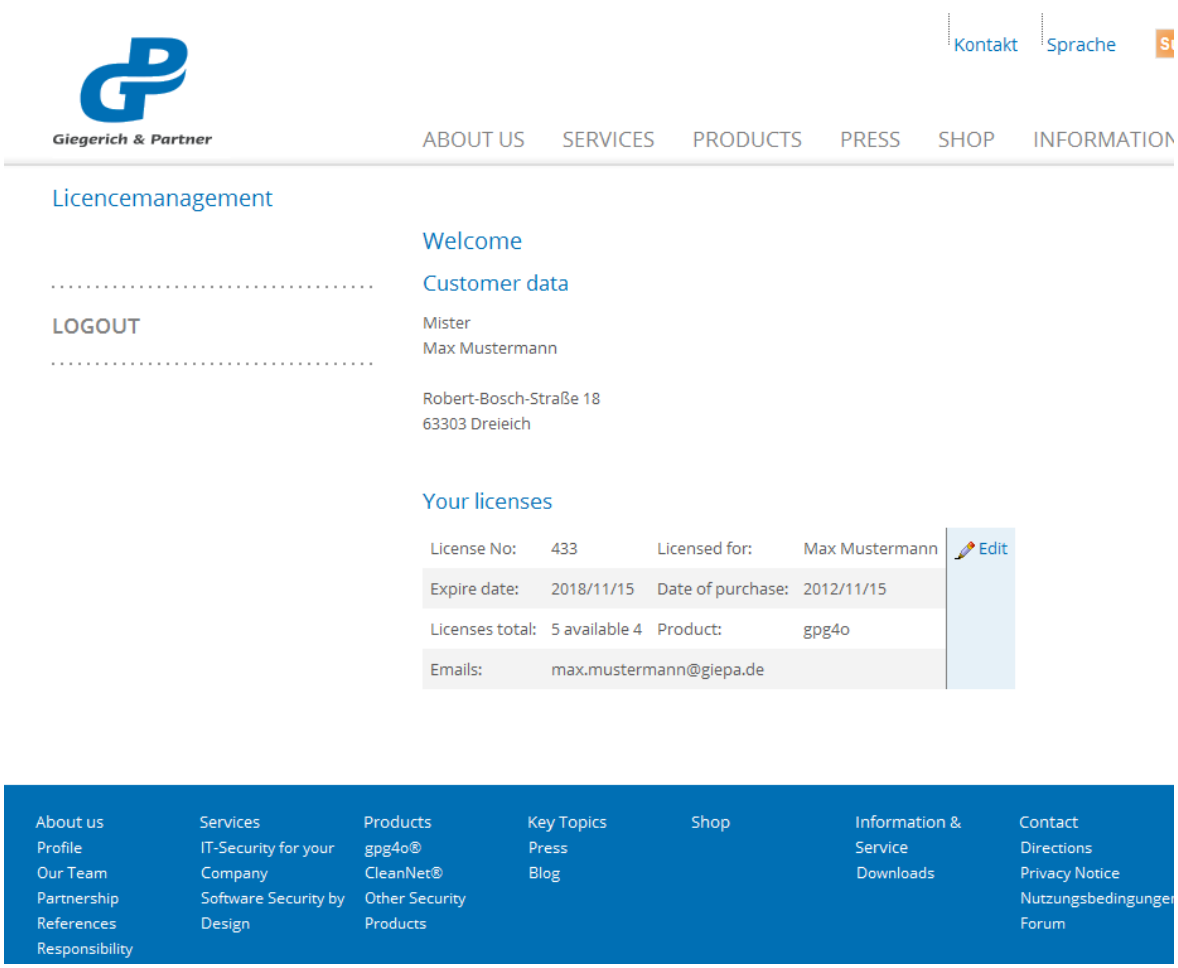
After having processed the online-ordering of **gpg4o** you can manage your licenses via our web interface (https://licmgmt.giepa.de/). For login you utilize the same access data that you use in our shop.



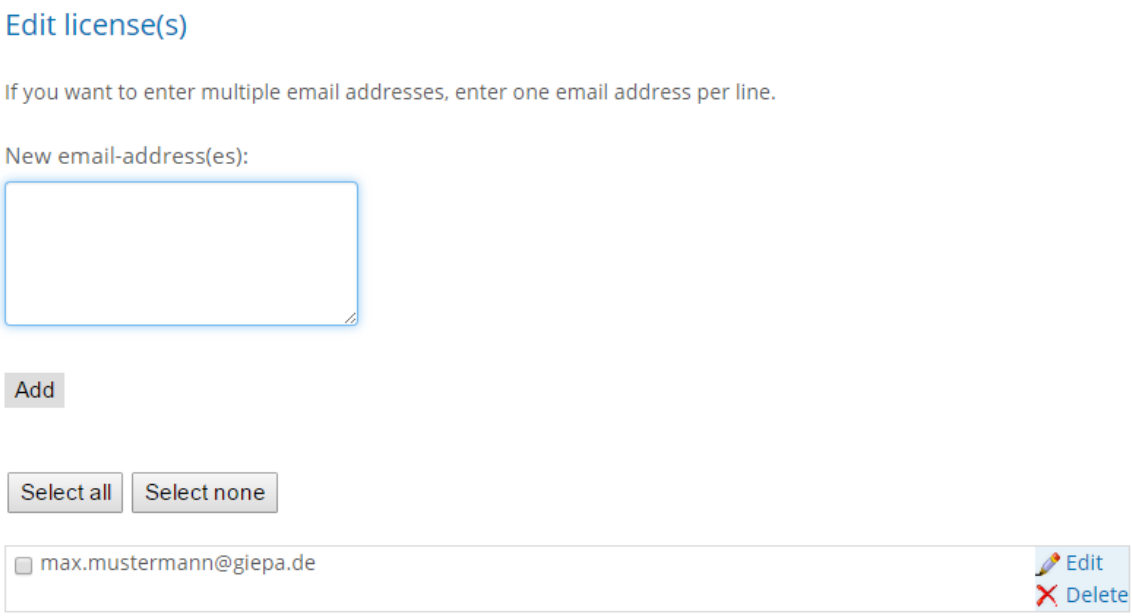
In the following menu you can see a summary of your licenses. You can see how many licenses are at your disposal altogether and how many of them are already utilized or which of them are still available.

Moreover, you can see the date until which updates will be placed at your disposal.

In order to make alterations to your licensing, click the pen-symbol **„Edit“**.



Now enter the email address you desire. In order to be able to enter several email addresses at once, separate them from each other with a new line. Email addresses which have already been entered can be individually adapted via the buttons **„Edit“** and **„Delete“**.



Subsequently, you can choose whether you want to download the license file directly or whether you want to have it sent by email. Alternatively, you can also define by check-marks to which email addresses the license shall be sent. Here, you can select individual addresses or all addresses.

Now you can import the license. For this purpose open Microsoft Outlook® and choose **„gpg4o – GPG for Outlook“** in the ribbon. There click the button **„gpg4o-Help“** and **„About gpg4o“**. In the information window appearing now click on **„Import license“**. A file selection dialog will appear. Browse to your license and choose **„Open“**. Now, your license file is imported and a corresponding message will appear which you can confirm by clicking **„OK“**.

It is also possible to import the license file once you have received it by email as file attach-

ment. For this purpose click the right mouse button on the file attachment and choose the item **„Import license for gpg4o“** in the context menu.

5.2 Period of Validity of the License

The license of **gpg4o** entitles you to the unlimited use of **gpg4o** with the licensed email address. The period of validity of the license starts with the first download of the license file. **gpg4o** is licensed for each real person. Therefore, **gpg4o** also works with only one license at several computers as well as with further email addresses within the same installation, as long as the licensed email address is configured within Microsoft Outlook® .

5.3 Period of Validity of the Product Maintenance/Support

During the period of validity of the product maintenance/support you will receive product updates with numerous new functions of **gpg4o**. Furthermore, you have the possibility to make use of the support via email **„support.gpg4o@giepa.de“** in case of questions or problems.

If the period of validity of the product maintenance/support has elapsed **gpg4o** can still be used. That means that you can continue to send encrypted/signed emails and read encrypted/signed emails as well. However, you do not have the possibility any longer to install new updates and to contact the support.

5.4 Extension of the Product Maintenance

The team of developers of **gpg4o** permanently improve the program and integrate customers' suggestions into new versions. With an extension of the product maintenance you may obtain new versions of **gpg4o** which were published after expiration of your product maintenance/support. In addition, you also extend the possibility of contacting the support via email. The period of validity of the product maintenance/support is extended by the number of purchased years of extension. Thus, the expiration date of the product maintenance/support is extended by the purchased years.

Example 1:

Original expiration date: 1st April 2015

On 1st February 2015 you purchase an extension of one year, in the first year after having bought **gpg4o**.

Expiration date after having bought the extension: 1st April 2016

Example 2:

Original expiration date: 1st April 2015

On 1st June 2015, after expiration of the product maintenance, you purchase an extension of one year.

Expiration date after the purchase of the extension: 1st April 2016

Here, you have a loss of 2 months of support and update.

Hint: After having purchased an extension this new, modified license file will have to be imported once into **gpg4o**.

6 Utilizing gpg4o

After having configured **gpg4o** and after having generated corresponding keypairs for your email accounts you will now have to send your public key to your communication partners. A keypair consists of two keys: One private-key and one public-key. When generating the keypair you were asked to enter a passphrase for the keypair.

Attention: **Never** pass your passphrase or your private key to another person! Each person coming into possession of your private key will be able to decrypt your emails and to sign new messages with your name.
You should keep the passphrase as safe as your other passwords and **never tell it to anyone else**.

The following brief example shows the general application of **gpg4o**:

Person A wants to make encrypted communication with person B. He therefore sends an email with his public key to person B and asks for his public key. This key exchange has to be done once for every contact partner.

Person B is now in possession of person A's public key and is therefore immediately able to send an encrypted answer. Person B will now answer the demand, attaching his public key and encrypting the answer with person A's public key.

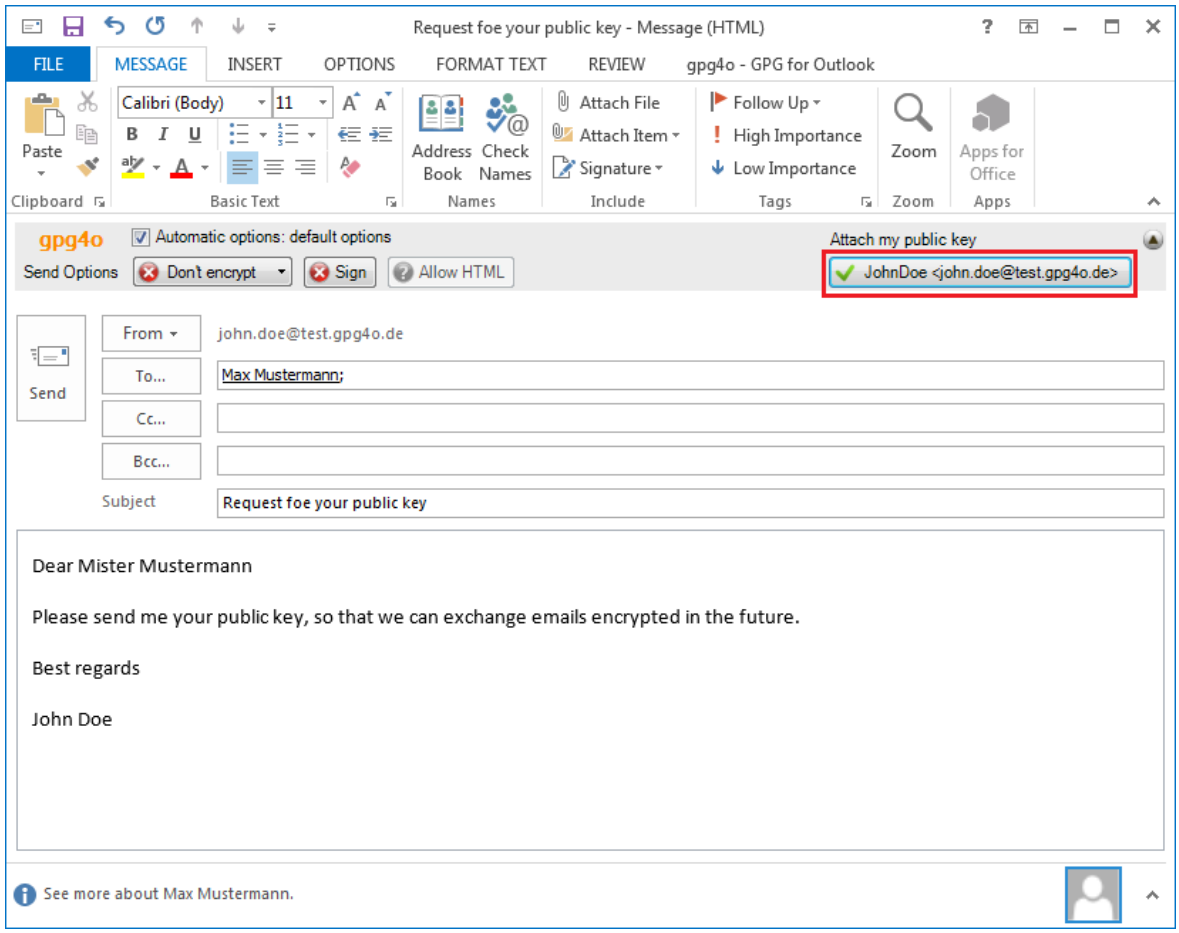
Person A then receives person B's encrypted email and decrypts said email with his own private key. Person A imports person B's public key and is now also able to encrypt to person B.

Hint: In order to be able to still read the emails sent by oneself, the own public key is always utilized to encrypt emails.

6.1 Sending Public Keys

In order to permit sending you encrypted emails you will have to distribute your public key to those persons which whom you intend to write encrypted messages in the future.

For this purpose you are kindly asked to generate a new email and to click the button below **„Attach my public key“**. In doing so, your public key will be enclosed with this email as attachment. If desired, place a checkmark in the button **„Sign“** in order to digitally sign your email. If your communication partner has already imported your public key it is not necessary to send the key another time.



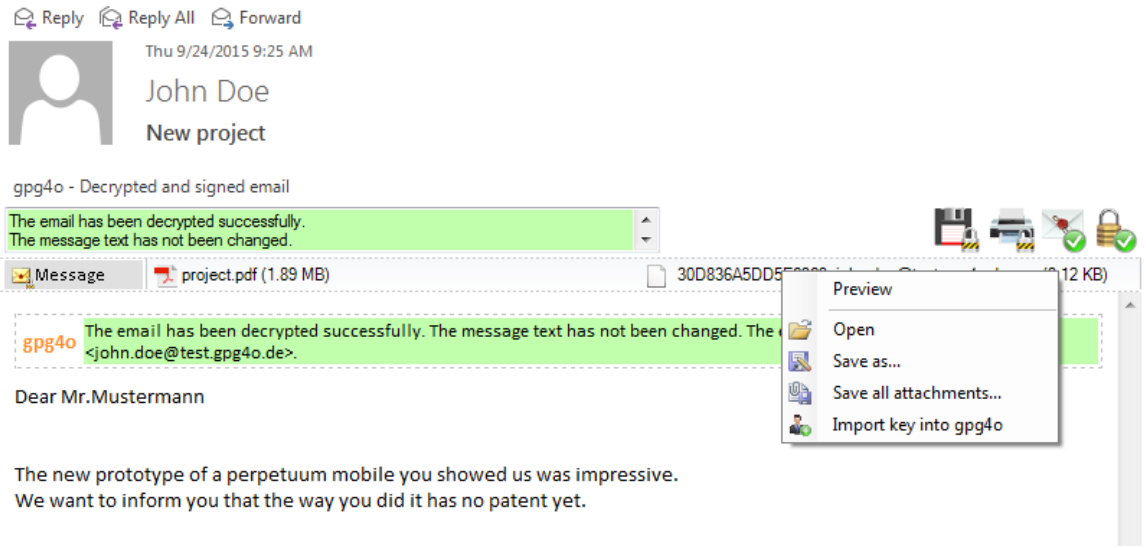
Please keep in mind that when directly sending emails, the standard options you have chosen will be utilized unless you have defined sending rules (see paragraph 8).

Hint: Pay attention whenever you are sending emails wether they should be encrypted or not.

The public key can be imported by all current encryption tools, which support the **OpenPGP**-standard. It only comprises the public part of the keypair, not the private one.

6.2 Importing Public Keys

If your communication partner sends you a key as an attachment of an email you may click the right mouse button and click the entry **„Import public key“** in the appearing context menu in order to import the key to your key management.

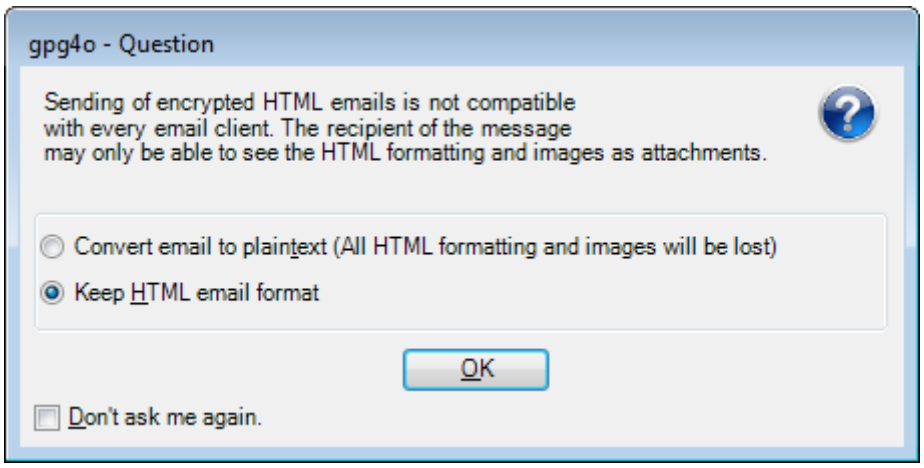


Alternatively, you have the possibility in the key management to import the key from a key-server (see paragraph 7.11).

As soon as you have imported the public key you can send encrypted messages to this person and also verify signatures of his emails. This exchange of the public key must be made once with every communication partner with whom you intend to exchange encrypted emails.

6.3 Sending Encrypted and/or Signed Messages

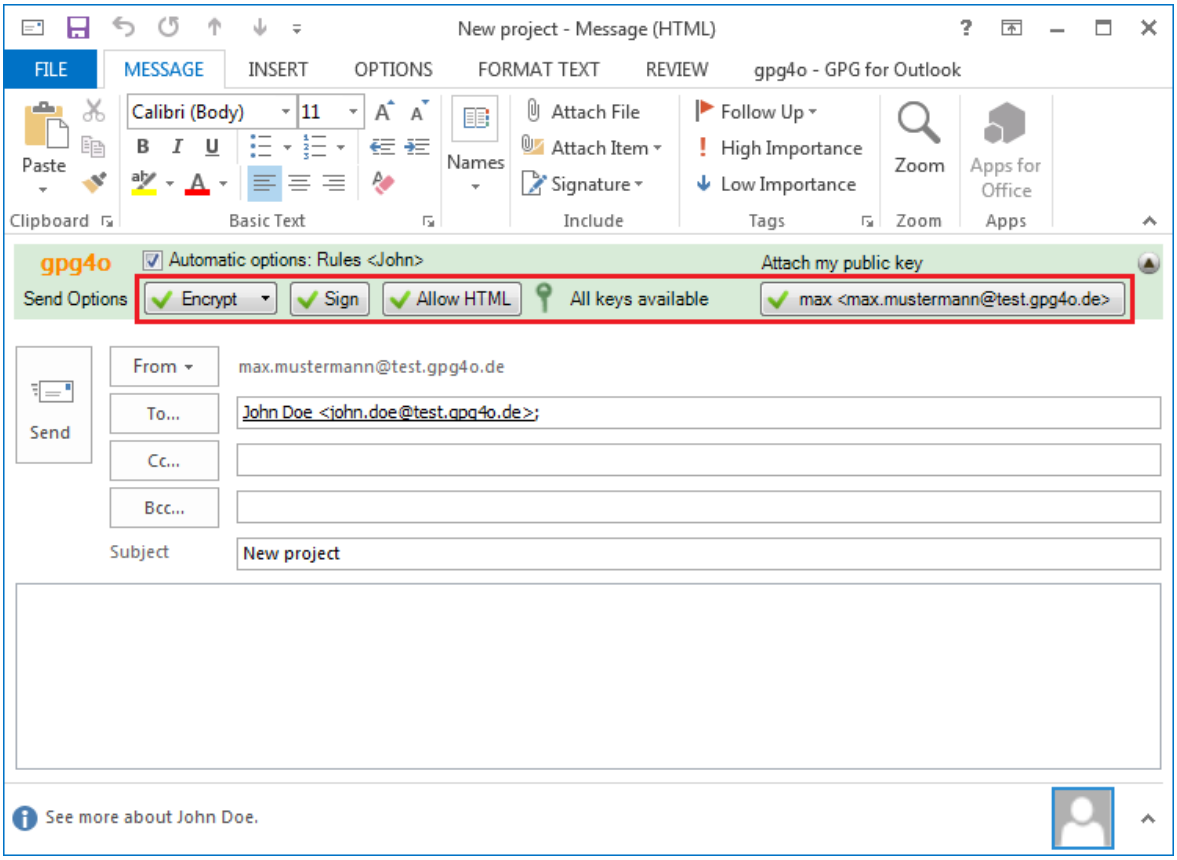
You can now send encrypted and/or signed emails. In order to guarantee the best possible compatibility with all current email programs you should write your emails in Plain-Text format. Of course, you also have the possibility of sending emails in HTML format. A corresponding selection possibility will appear as soon as you choose the option **„Encrypt“** or **„Sign“**.



If you want to define your selection as default you will have to enable the checkmark **„Don’t ask me again“**.

Hint: In the account settings (see paragraph 9.3) you can reset this option.

If you write an email the **gpg4o** send options will be displayed to you under the menu ribbon.



Here, you can define whether your emails shall be encrypted and/or signed and whether your public key shall be attached to the email.

Before sending an email enable the button **„Sign“**, if you want to send it signed or **„Encrypt“**, if you want to send it encrypted. If you enable both buttons your email will be sent encrypted and signed.

Please also pay attention to the status **„Encrypt (only attachments)“**, which is selected by pressing the button **„Encrypt“** again. This status can also be combined with **„Sign“**, in this case, however, the message will only be signed while the attachments will be encrypted and signed.

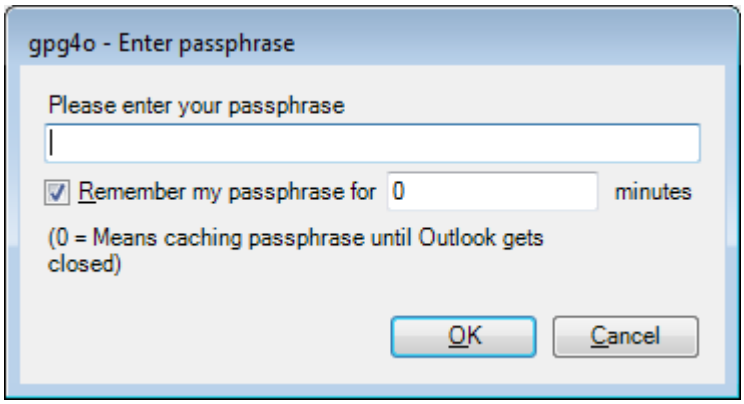
Furthermore, the send options will show you whether you have all required public keys for the recipients of the email. However, this will only be done if the send options **„Encrypt“** or **„Encrypt (only attachments)“** are active.

If all public keys for the entered recipients are available this will be symbolized by a green key in the send options bar. If you do not have all public keys this will be shown to you by means of a red key.

If you have entered a keyserver in the setting **„Autoimport“** (see paragraph 9.6.2) the

missing keys will be searched on the indicated server and will be imported automatically into your keyring.

After having written the message completely and having selected the send options, click **„Send“** as usual. If there are problems when sending the email (like unusable keys) you will be notified by **gpg4o**.



If you have selected the message to be sent signed you will now be asked to enter your passphrase. For this purpose please use the passphrase which you have selected for your key during the configuration of **gpg4o**.

Hint: For all actions requiring the utilization of your private key you will be asked for your passphrase. If you permit **gpg4o** to remember the passphrase you will only be asked for it again if the indicated period of time has elapsed since the last utilization of the private key.

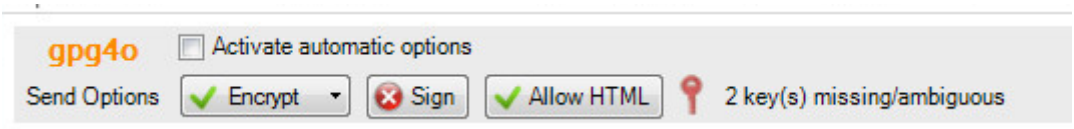
Actions requiring the private key are as follows:

- Signing messages, attachments or keys
- Decrypting of messages and attachments
- Generating revocation certificates
- Modification of the passphrase
- Adding Identities
- Setting the primary Identity

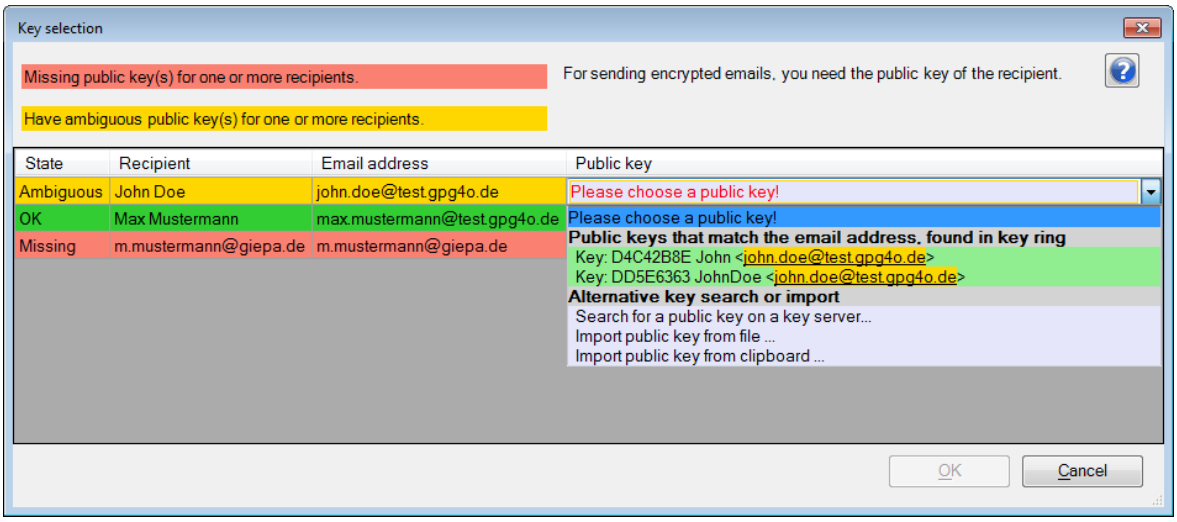
6.3.1 Manual assignment of keys

While composing an encrypted email it will be shown, if there is a appropriate key available for every recipient. If there is an autoimport-keyserver configured, it will be used to search for missing keys and if a suitable key was found, it will be imported automatically.

If no appropriate key was found, neither in your keyring nor the keyserver, this will be shown with a red key in the send options panel. If this key is green, then the appropriate key for every recipient could be determined.



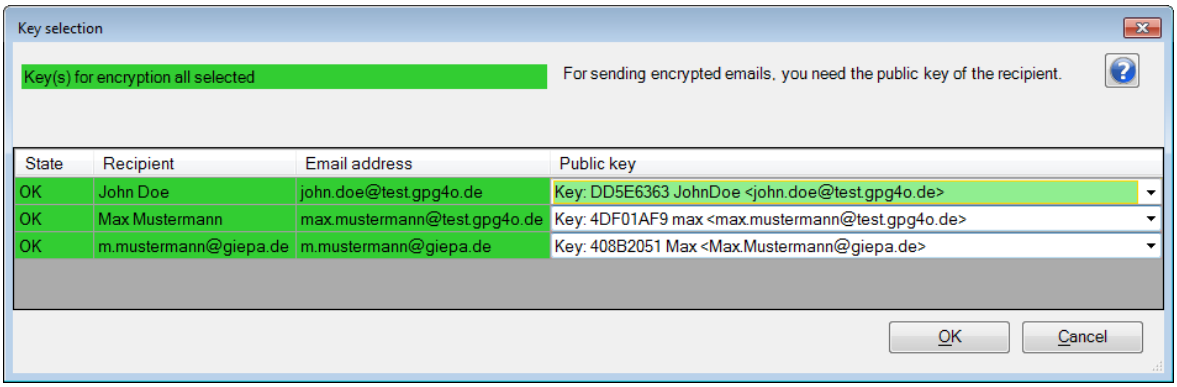
With a click on the key symbol or on the text alongside the symbol, the key selection dialog will be opened. Here you are now able to assign a specific key to a specific recipient manually.



Here the background of the email addresses is colored according to the following system:

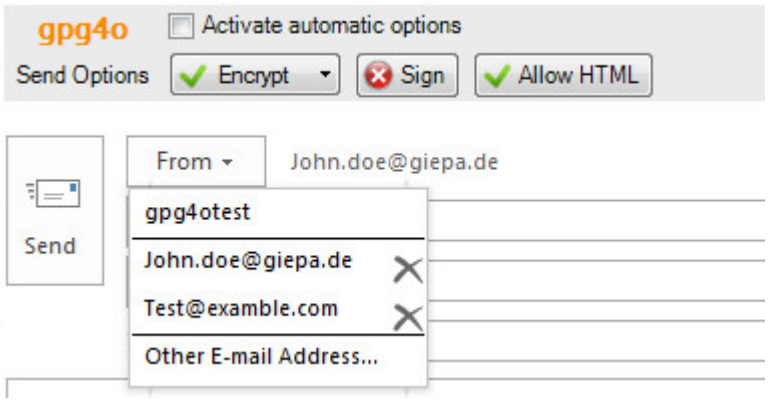
- Green: An appropriate key is available
- Yellow: There are at least two appropriate keys available
- Red: No appropriate key available

Now you can assign one or more keys to the different email addresses.



If each email address has been given a key and none of the lines are marked red or yellow, you can close the Dialog by clicking the button **„OK“**. The email can now be encrypted and sent.

6.3.2 Virtual Accounts

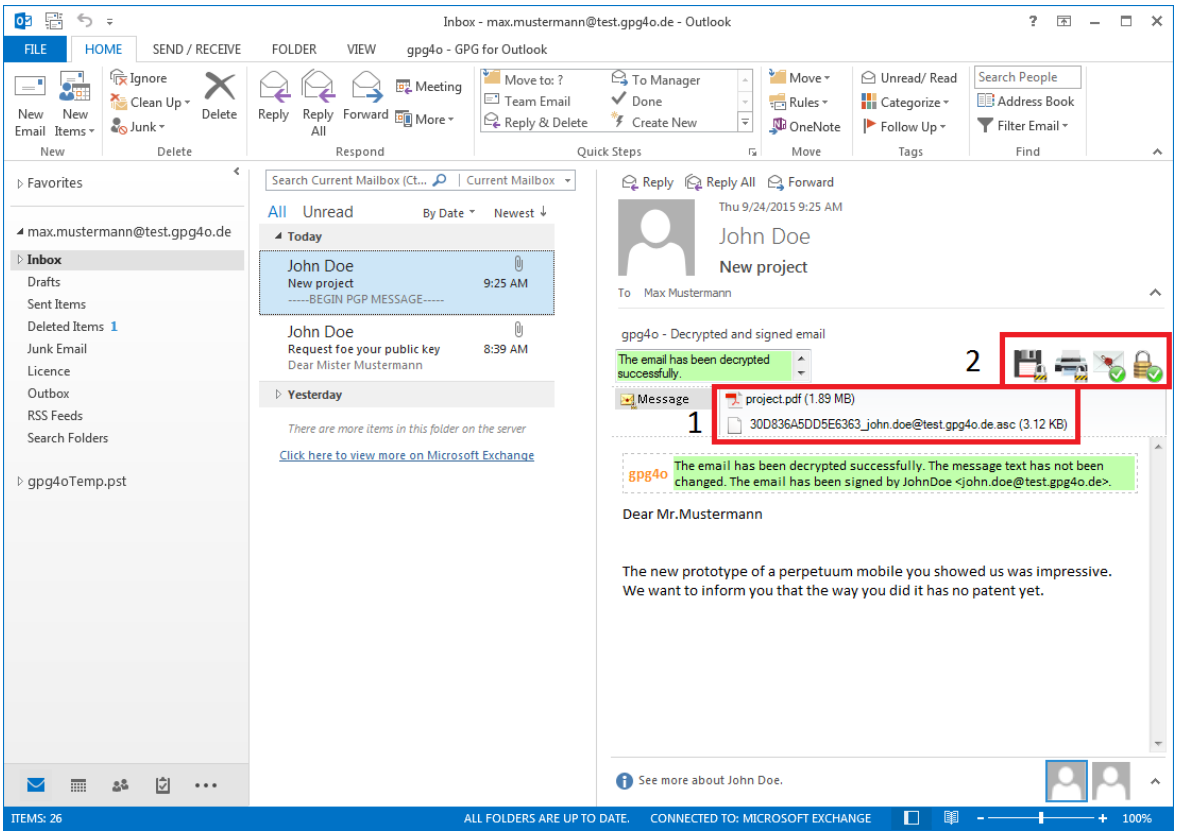


While composing a new email you can select from which account you want to send your email, by clicking on the **„From“** button. For every email address listed there, **gpg4o** will create a virtual account. This virtual account can be configured in your settings by opening the account management. (see paragraph 9.3) Therefore you are able to use **gpg4o** for every single virtual account.

Hint: If an email address is deleted inside the **„From“** field, the corresponding virtual account will be deleted.

6.4 Receiving of Encrypted and/or Signed Messages

If you receive an encrypted and/or signed email another pane will be shown below the reading pane. Here, you can now read the emails decrypted or without signature blocks.



1. *Decrypted attachment and public key of Mr. Doe*
2. *Actions and decryption status*
   - Save email decrypted
   - Print preview
   - Signed
   - Encrypted / Forget cached passphrase

The symbols signalize whether the email was received as encrypted or signed email. Here certain actions (see 2) are at your disposal. For example you may save the message permanently decrypted or open the print preview of the decrypted message (see paragraph 6.7). For this purpose simply click the corresponding symbol.

The colored box on the left shows information about the validity of the signature and status of the encryption.

Three colors are used to be able to see the status faster:

- **Green** means that the email was correctly encrypted. If the email was also signed, this color shows that the body and attachment were not changed in the sending process.
- **Turquoise** means that the signed key is unknown or the key has not been validated/signed. (see section 7.10.3)
- **Red** means that the email could not be decrypted or the message and/or your attachments have been changed during the exchange.
- **Yellow** means that the senders address could not be found in the identities of the key.

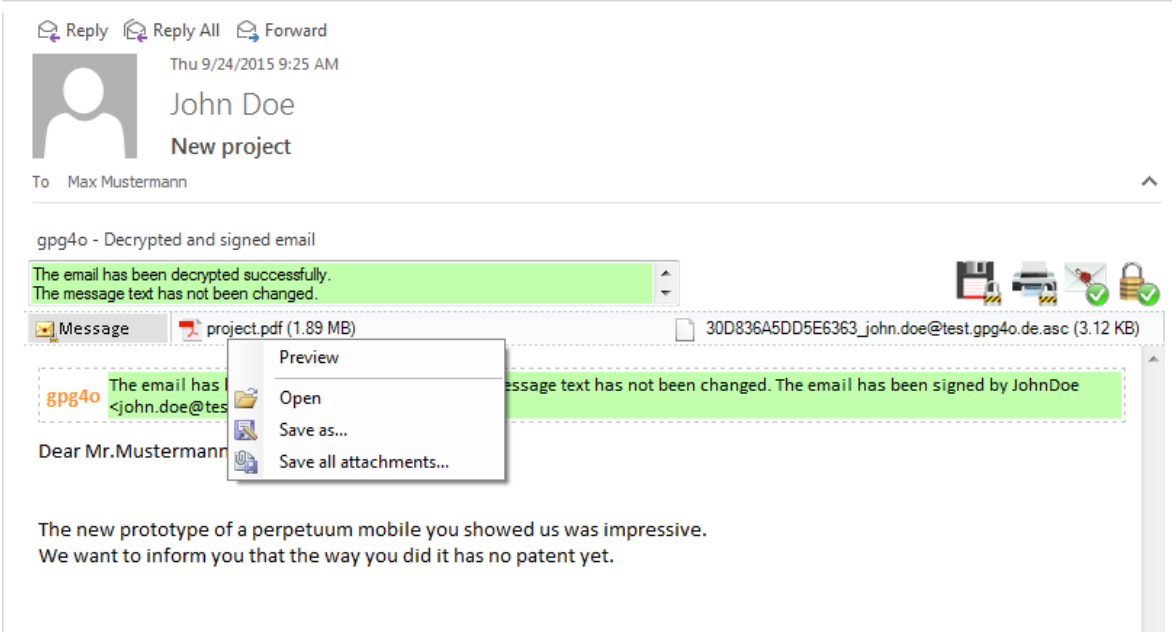
Not only does **gpg4o** check if the message has been changed, but also if the email of the sender fits to the signed key. This check compares the email address of the sender and the identities of the signing key.

If the senders address is not in the identities of the signing key, then the status display is highlighted in **yellow**.

6.5 Sending and Receiving Encrypted Attachments

As soon as you send an encrypted email which contains an attachment **gpg4o** will do the rest for you quite automatically. You can attach files to your emails as normal without having to worry about the details. As soon as the check mark is placed with **„Encrypt“** all attachments will be encrypted as well in addition to the text of the email.

If you have received an encrypted email with attachment you can either save the encrypted attachment or open it directly. For this purpose the context menu (Click right mouse button on the attachment) offers you the options **„Preview“**, **„Open“**, **„Save as...“** and **„Save all attachments...“**.



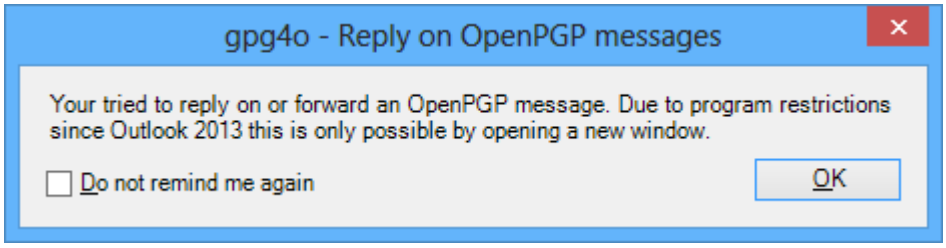
Alternatively, you may also save the attachment in a folder by drag and drop.

With the option **„Preview“** or with a simple click on the attachment it will be shown in the display as you know it from Microsoft Outlook® .

6.6 Reply/Forwarding of emails in Outlook 2013 onwards

If you want to answer or forward an encrypted email in Microsoft Outlook 2013® or Outlook 2016® , the answer to be written will not open in a window of its own by default. Thus, there will not be all functions of **gpg4o** at your disposal. In order to be able to make use of all functions the email has to get a window of its own. If this occurs **gpg4o** will point it out to

you.

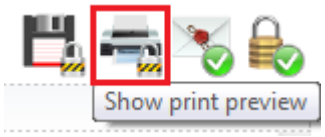


If you do not want to be informed of this fact again place the check mark with **„Do not remind me again“**. Via the button **„OK“** you continue the action.

6.7 Printing Encrypted Messages

For printing an encrypted message, said message has to be decrypted before (see paragraph 6.4).

Having done that you have two possibilities of printing your decrypted message. If you have your reading pane on the right side you can print the email by clicking the symbol **„Print preview“**.

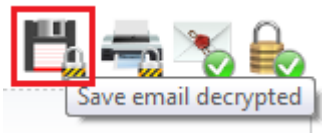


Otherwise you can also open the email by double-click and print it there as usual with the button combination Ctrl+P or by clicking **„File“** and then **„Print“**.

Hint: In the test version printing of encrypted messages is not possible via the button shown above.

6.8 Permanent Decrypted Saving

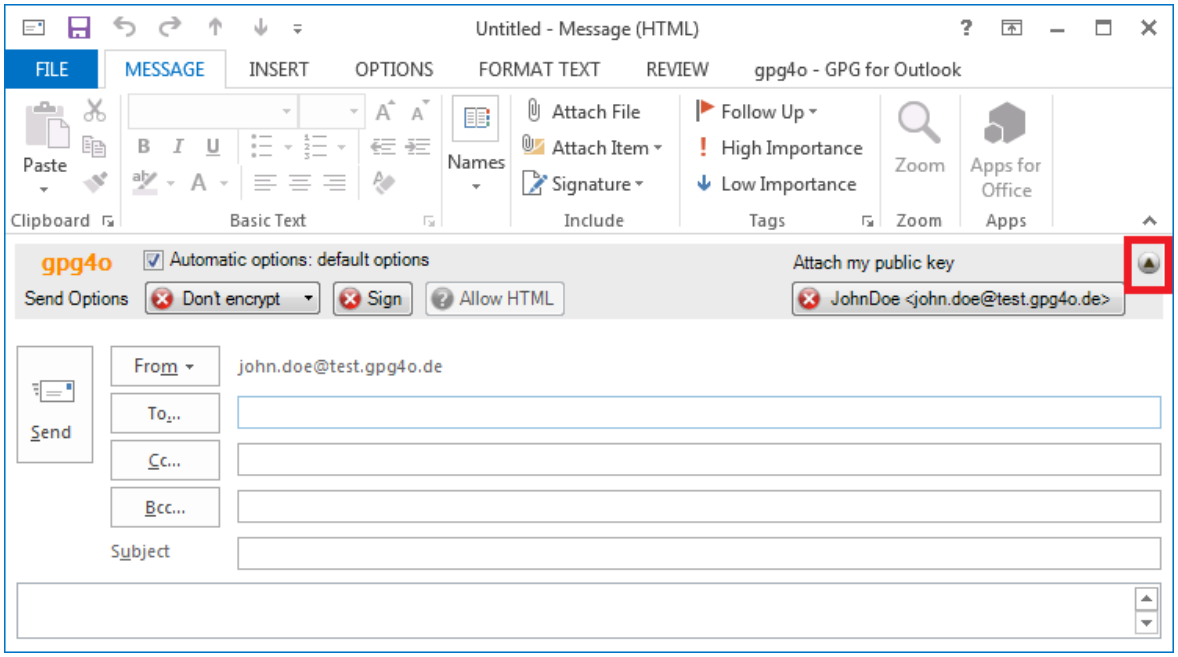
For simpler archiving **gpg4o** also offers the possibility to save messages with permanent decryption.



For this purpose click the symbol **„Save email decrypted“** in the reading pane of **gpg4o**.

Attention: If the email is still located in a synchronized folder the message will become also readable on the server. You should therefore utilize this function with corresponding care. Please note that this feature is not available in an **Home & Student Version**.

6.9 Hide Send Options



In order to put more space at your disposal for the email editor you can fold up the send options or hide them completely.

If **gpg4o** is enabled for utilization with an account you can fold up the send options via the button with the arrow in the right upper corner of the send options bar and also fold it down again.

The send options remember the last state so that when creating another email they will be displayed to you in the same way as before.

If the account is not configured for utilization with **gpg4o** a button will be shown instead of the arrow with an **„X“**. If you click on it the send options will not be shown any longer in the future in case of inactive accounts.

You can undo this in the settings on the page **„View“** (see paragraph 9.1.3).

7 Key Management

With the key management of **gpg4o** you can manage the keys generated or imported by you. You can also look at all key details, generate new keys, revoke old keys, delete and much more.

7.1 General Information Regarding Keys

As we often use some **OpenPGP**-specific terms we would first of all like to give you a brief explanation of those terms.

Every **„Keypair“** consists of a private and a public key. The public key is calculated from the private key, inversely, however, this is not possible. That is why you as a key owner always own the public and the private key, your communication partners, however, only have your public key.

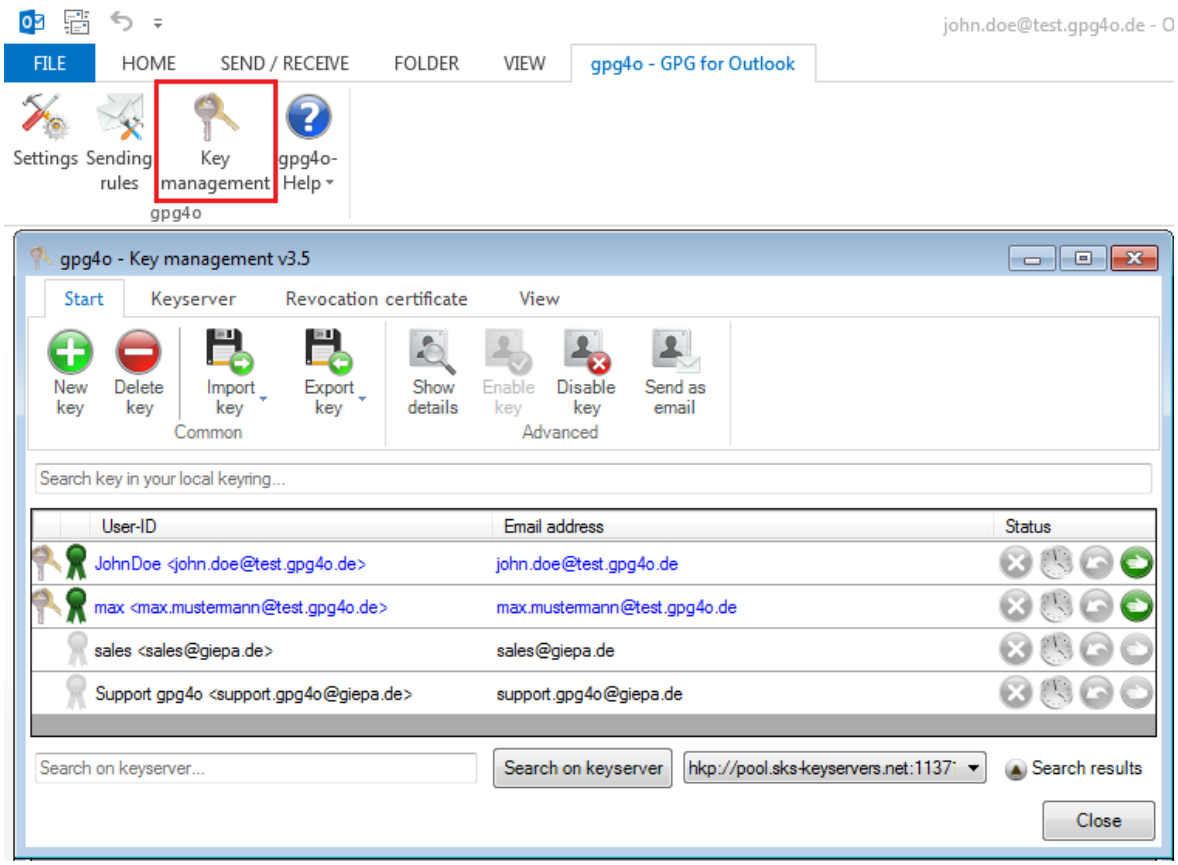
Your communication partners encrypt messages to you with your public key. You then decrypt them again with the private key. For signatures the principle is exactly the other way around. You sign a message with your private key, the recipient checks the signature with your public key.

In addition, every key comprises one **„Primary key“** and an optional number of **„Subkeys“**. If you generate a key with **gpg4o** one subkey will always be generated as well, other **OpenPGP** applications, however, can generate a much greater number of subkeys. In **gpg4o** they will only be indicated for the sake of completeness, for you as a user, they actually have hardly any importance.

Furthermore, a key is provided with one or more **„User-IDs“** which corresponds to a description of the key which can be read by human beings. Such a User-ID usually consists of the owner's complete name and his email address. As one key may have more than one User-IDs it can also be utilized for more than one email address.

7.2 Overview

In order to open the key management of **gpg4o** please click **„gpg4o - GPG for Outlook“** in the menu ribbon of Microsoft Outlook® and then **„Key management“**.

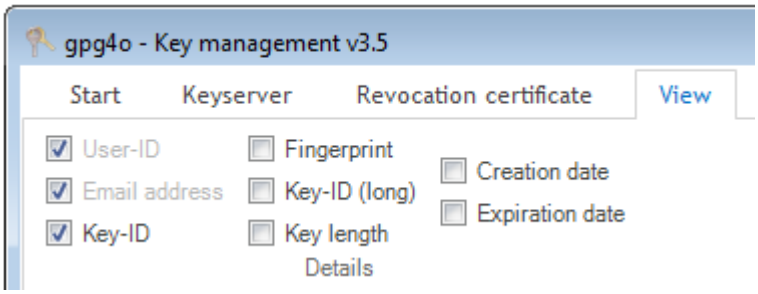


In the overview you can see all the keys which are contained in your keyring. Here, your own keys as well as imported keys will be displayed to you.

Most actions can be performed in several ways. The two most important methods for performing an action are the menu ribbon in the upper section of the key management and the context menu which you get to when clicking the right mouse button on the selected key(s).

Furthermore, many actions can also be applied simultaneously for more than one keys. To this end simply select several keys with the button Ctrl and select or deselect further keys.

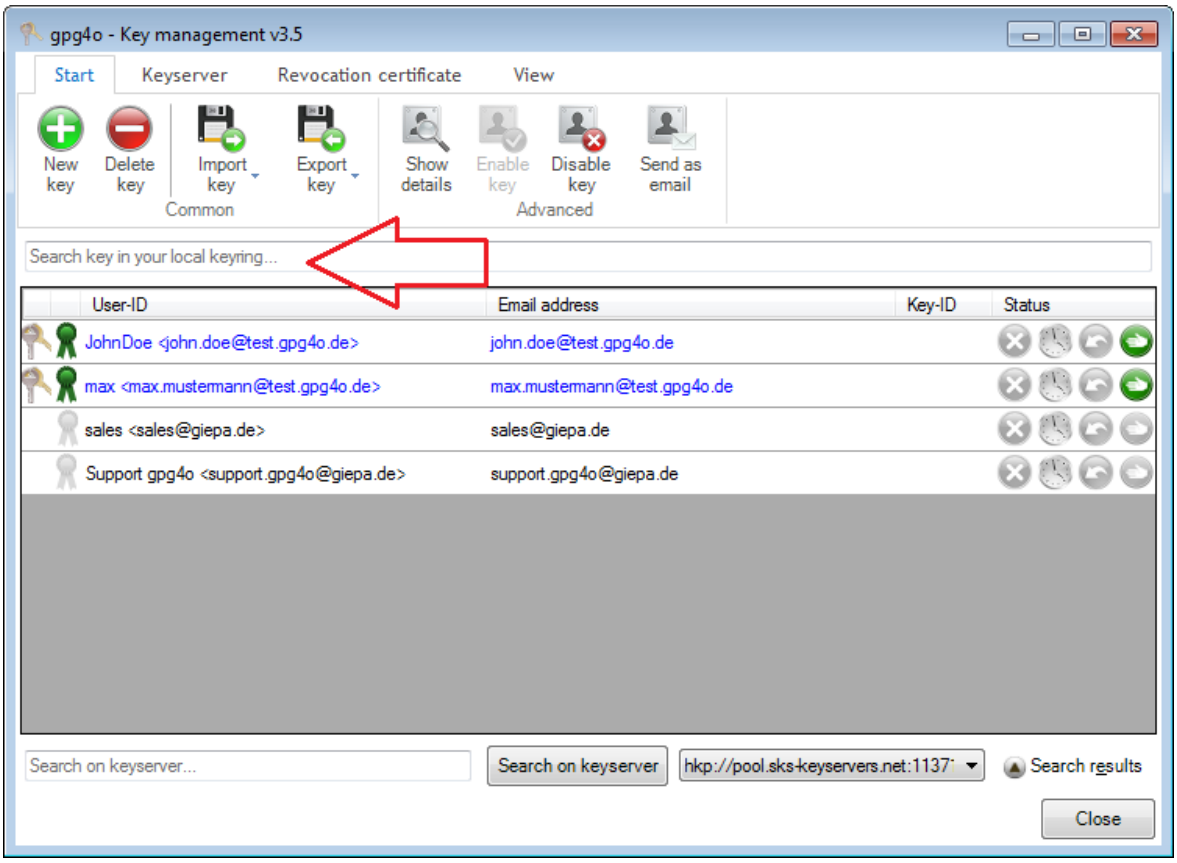
7.3 Modifying View



In the menu ribbon of the key management you can set via **„View“** which columns you want to show or hide, respectively.

Moreover, the columns can be sorted. If you want to sort the view by means of a column, simply click the column title. Every further click on the same column reverses the sorting.

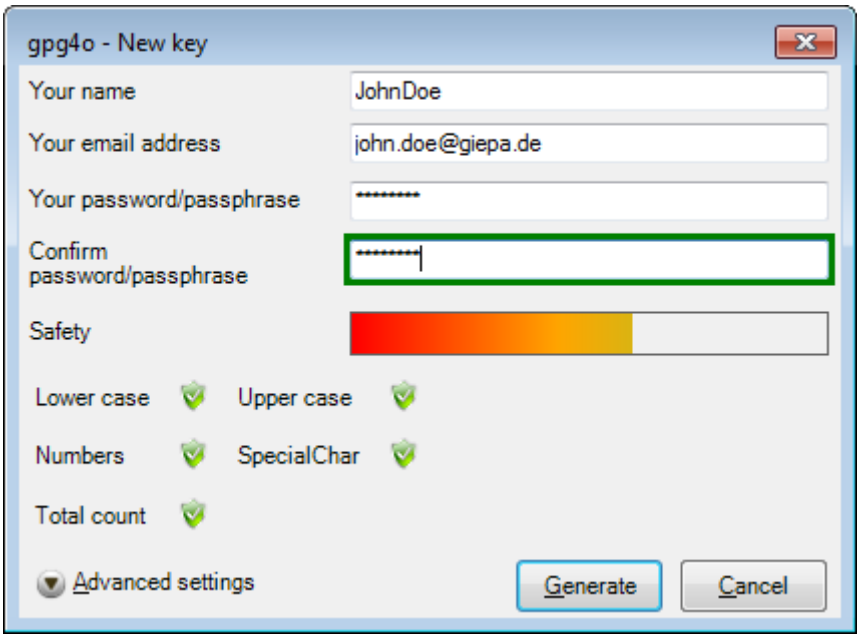
7.4 Filtering Keys



In addition, you have the possibility of filtering the view. For this purpose enter a search term into the field **„Search key in you local keyring...“** in order to show only suitable keys. Such a search term may be an email address or a name for example or only a part of it.

7.5 Generating New Keys

In order to generate another keypair, please click the option **„New key“** in the menu ribbon **„Start“**. In the dialog appearing then please enter the required data as you have already done when configuring **gpg4o**.



If you want to set further options such as the expire date for the new key please click **„Advanced settings“**. As soon as you have entered all required data, click **„Generate“**.

Hint: The generation of the keypair may take a little time.

7.6 Deleting Keys

In order to delete a key you have to select it and choose the option **„Delete key“** in the menu ribbon **„Start“**. Alternatively, you can press the button **„Delete“**.

Attention: Please mind that the deletion of a key is irreversible. However, you can import a key again which you have exported before.

Hint: If you delete a keypair, the private as well as the public key will be deleted. If the keypair to be deleted is stored in the **gpg4o** settings of an account this setting becomes invalid. In this case **gpg4o** will open the settings dialog after deletion in order to permit you the selection of another keypair.

7.7 Enabling/Disabling Keys

If you disable a key it will not be used for encrypting any longer. This makes sense, if you have more than one public key for the same email address of one contact if, however, you only utilize one of the public keys for encrypting. All further actions will remain unaffected.

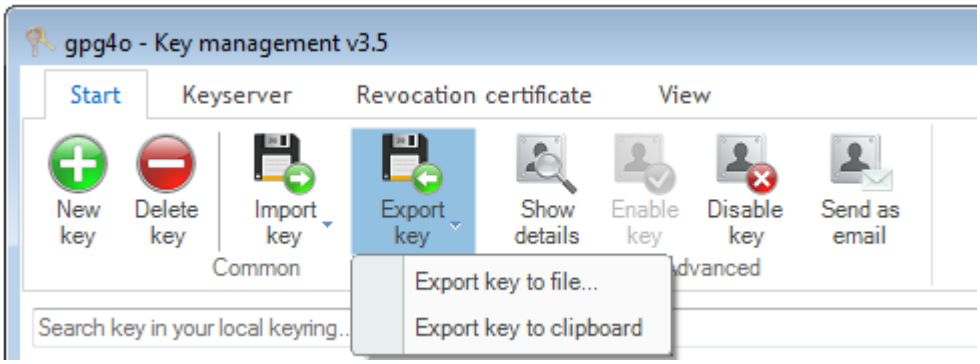
For disabling one or several keys you select them and click in the menu ribbon on the button **„Disable key“**. Contrarily, you can enable those keys again which you have disabled before by means of the button **„Enable key“**.

Hint: If the keypair to be disabled is stored in the **gpg4o** settings for one account this setting will become invalid. In this case **gpg4o** will open the settings dialog after disabling in order to let you select another keypair.

7.8 Exporting Keys

Apart from the sending of your own public key (see paragraph 6.1) you can export your own keys or those of your contacts, respectively, here in the key management, too.

Choose the key(s) you want to export and click on **„Export key“** in the menu. You can export the key(s) into the file system or into the clipboard.



An export into the file system is logical if you want to transfer the key(s) to another computer or onto your smartphone.

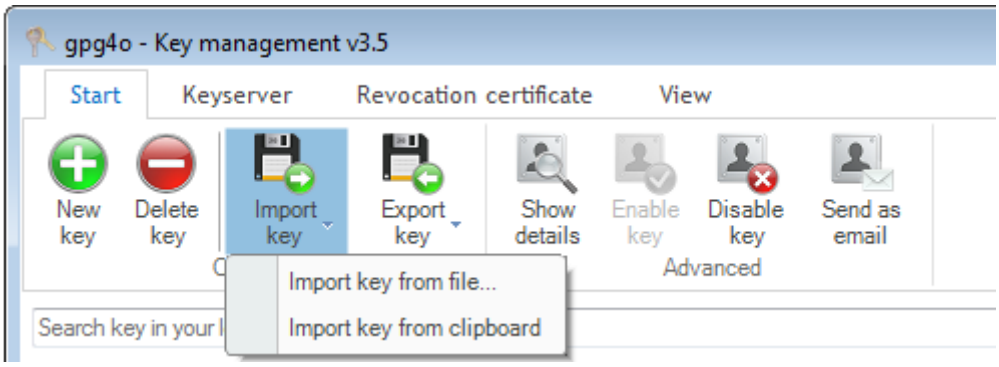
You will be asked where you want to save the key if you have selected **„Export key to file...“**. As soon as you have selected a folder where the key should saved, please click on **„OK“**.

Copying to clipboard is useful if you want to use the key(s) in a different program, website, or article on the internet without having to use a separate file.

If you have selected **„Export key to clipboard“**, the keys are copied to the Windows clipboard and you can paste the keys into any textfield by pressing Ctrl-V.

7.9 Importing Keys

You can also import a key into the key management. To do this, click on the button **„Import key“** in the menu and choose the option **„Import key from file...“** or **„Import key from clipboard“**.

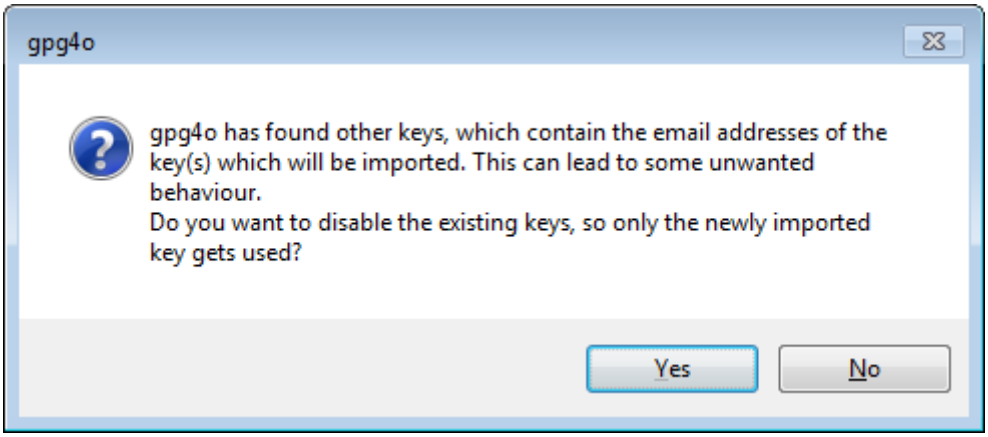


Public keys can be published on websites in text form. To import these keys into your own key ring, highlight the text and copy it with Ctrl-C. Afterwards, you can easily import the key with **„Import key from clipboard“** and use it.

If you have selected **„Import key from file...“**, a dialog will appear in which you can choose a key file to import. The selected key will be imported when you click **„OK“**.

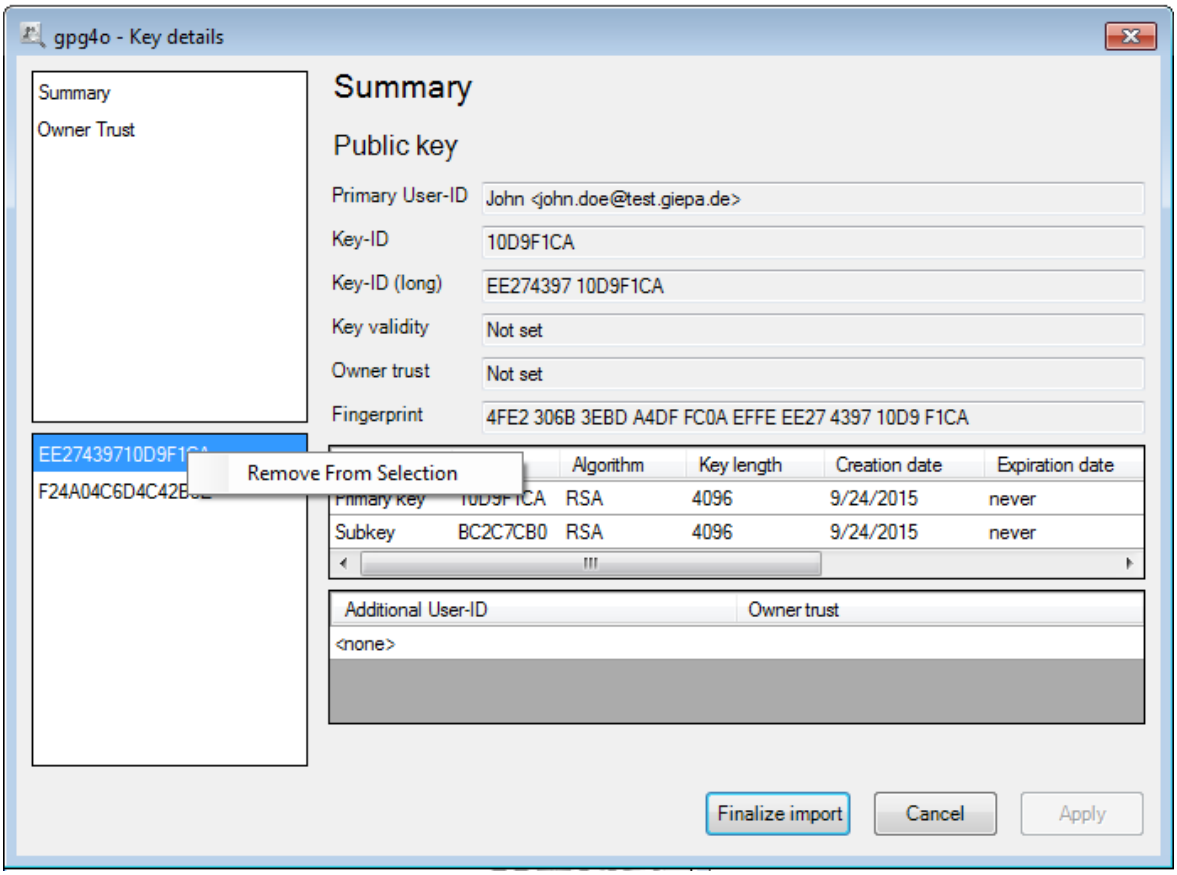
Tip: You can also import keys from the file system per drag and drop.

If one of the keys to be imported was issued for an email address for which you have already imported a key, you will be asked again as a precaution whether you want to disable the already existing key before importing the new one.



If the same key is concerned you do not need to have any more worries as differences between the keys will be automatically consolidated.

Afterwards, a summary will appear of the keys to be imported containing all necessary information.

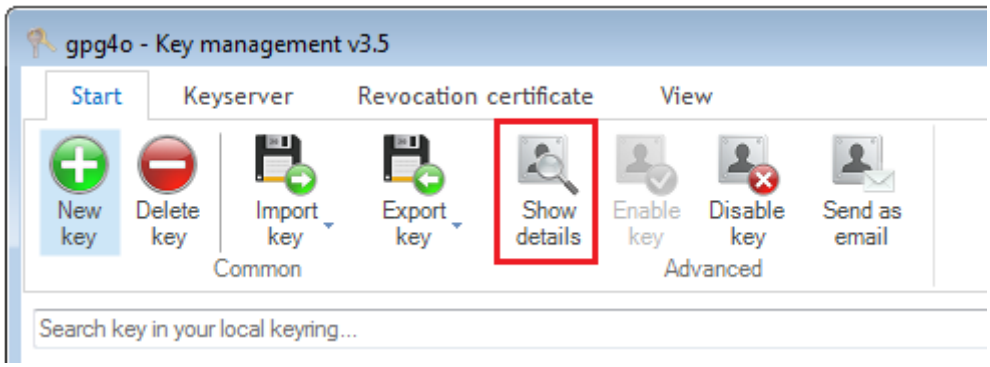


Here, you can still exclude individual keys from being imported if necessary by clicking the right mouse button on the key to be excluded and by clicking **„Remove from selection“**. You can also determine the owner trust for the key to be imported (see paragraph 7.10.5). For this purpose click the menu item **„Owner trust“** first and select the new owner trust for the keys there.

In order to finish the import of the key(s) click **„Finish“**.

7.10 Key Details

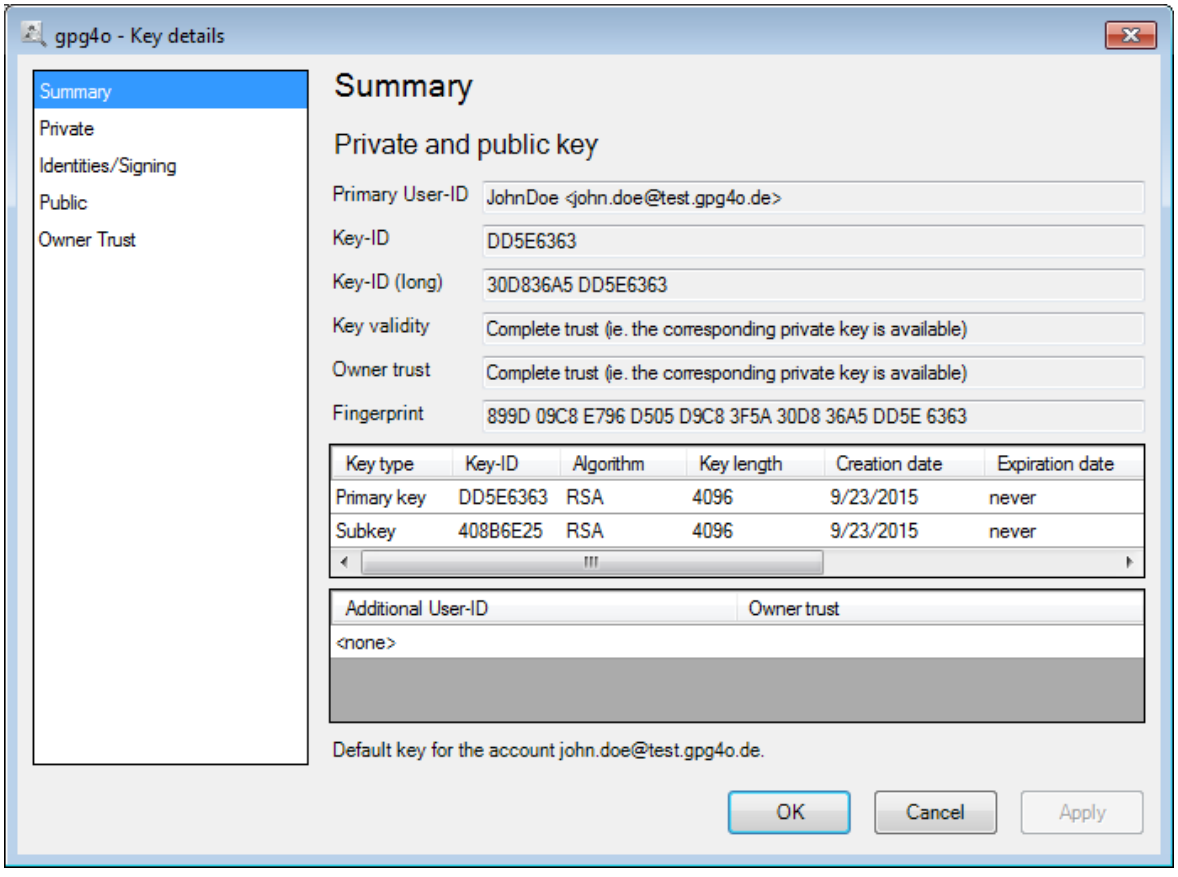
In order to look at one or more keys in detail you can click **„Show details“** in the menu ribbon **„Start“** or you press the right mouse button on the selected key(s) and click **„Details...“** in the context menu.



The key details have been subdivided into several sections which are listed on the left side in the menu. The section **„Private“** is only visible for keypairs. In order to change to another section simply click the name of the section.

7.10.1 Summary

On the summary page you can see the most important information with regard to the selected key. The **„Key-ID“** and the **„Fingerprint“** identify the key, the Key-ID being a short form of the fingerprint. The fingerprint should be synchronized during the exchange of the keys, best by telephone (see paragraph 7.10.3).



Additionally, the **„Owner Trust“** and the **„Key Validity“** are indicated. You can define the owner trust yourself (see paragraph 7.10.5), the key validity will be determined by means of already existing signatures and the owner trust of the signee.

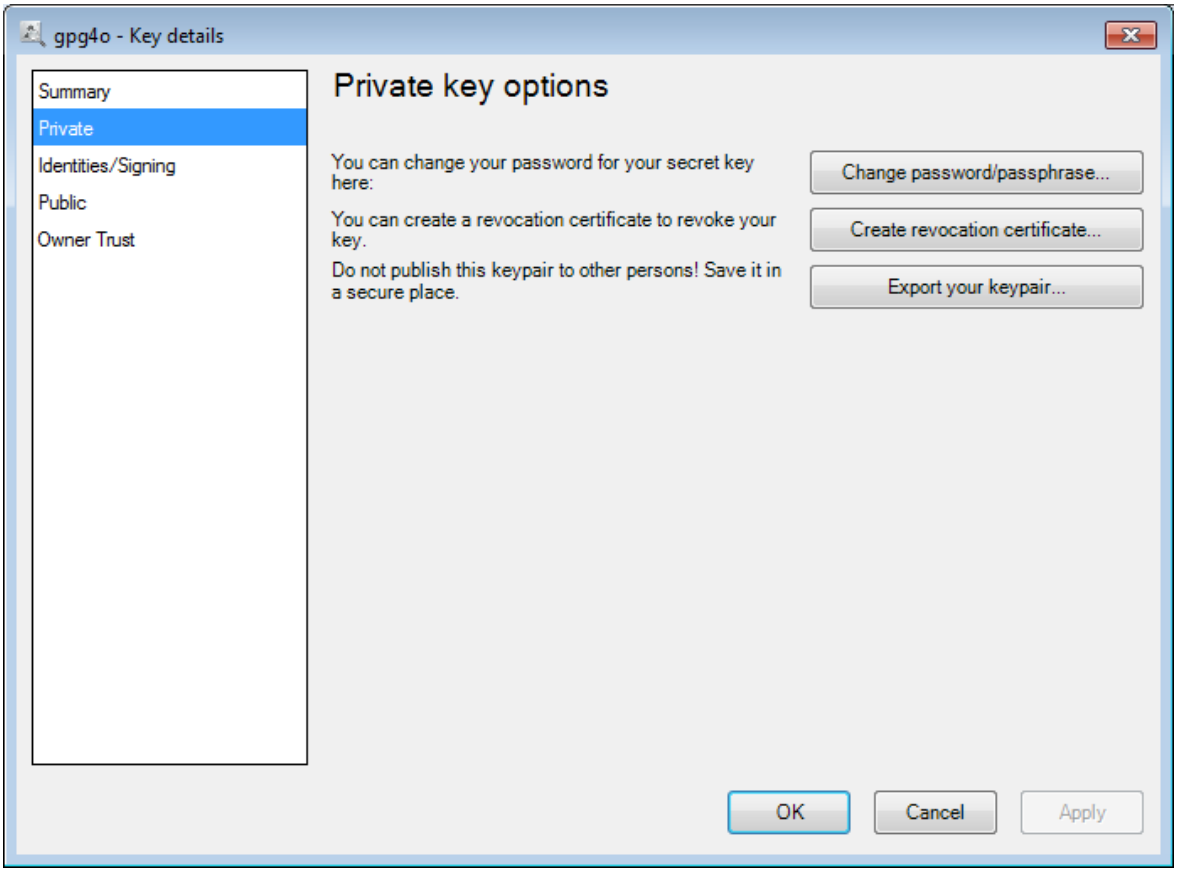
The term **„Key Validity“** means whether a key has been identified as valid by own signatures or by those of trusted keys. Here, the **„Web of Trust“** also plays an important part.

A key is valid if it

- Was signed by one of your own keys
- Was signed by another key owner whom you trust fully
- Was signed by at least 3 other key owners whom you trust marginally

7.10.2 Private Key

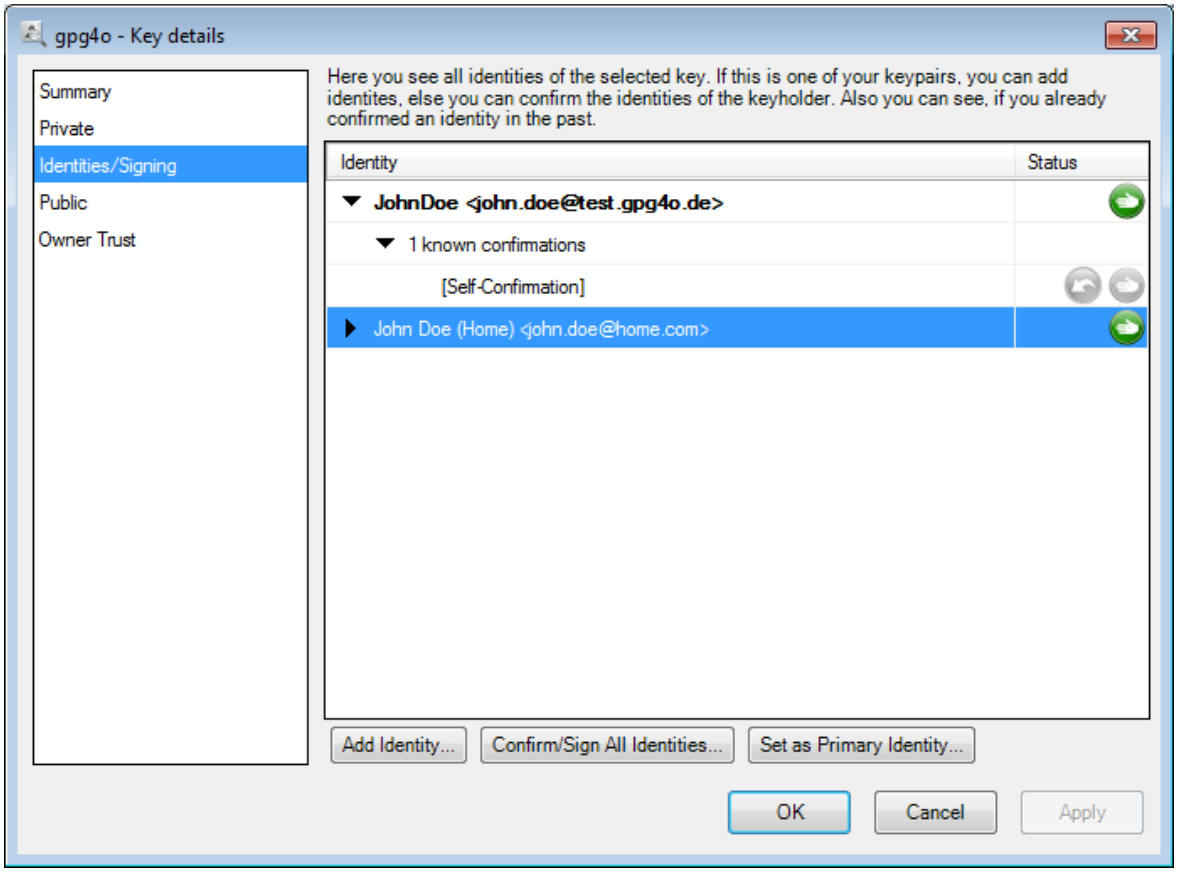
If you open the section **„Private“** in the details of a keypair, you can modify the passphrase of the key, generate a revocation certificate or backup the complete keypair.



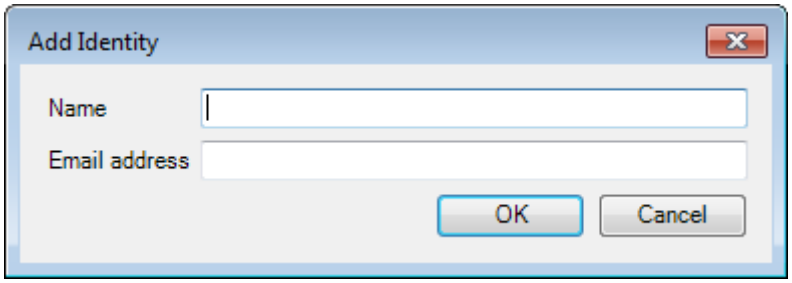
Attention: You should **never** give the data backup with your private key or the revocation certificate to anyone else.

7.10.3 Identities/Signing

In this area, all of the identities (User-IDs) for the given key are displayed. For key pairs, you can add an identity or choose a main identity. Furthermore, you can confirm an identity (sign) and hereby validate it in case you have disabled the option **„Always treat all keys as valid“**. (see paragraph 9.9.1)



To give a new identity a key pair, click on **„Add Identity...“** and enter the name and email address for the identity. Clicking on **„OK“** creates a new identity for the key.



If you have disabled **„Always treat all keys as valid“** in the options, or want to validate a public key and all of its identities, click on the button **„Confirm/Sign All Identities...“**

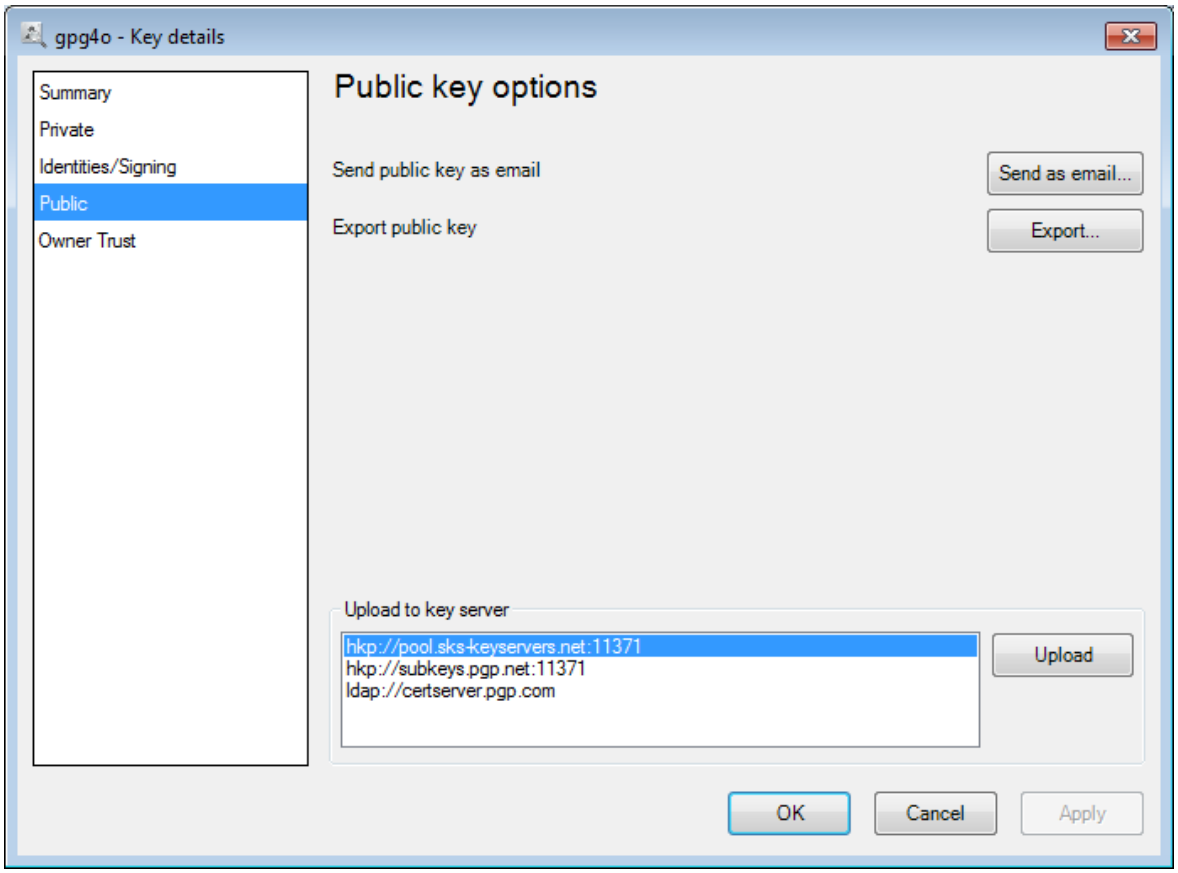
Afterwards, indicate how sure you are about the authenticity of the signed key. With this selection, the strength of the signature is determined. Clicking on **„OK“** will apply the signature of the key.

Hint: To be sure that the key belongs to the given person, you should compare the fingerprint. This is best done by phone, since emails can be faked by **„Man-in-the-Middle“** attacks.

All programs that work with **GnuPG** show the primary identity of a key. You can change the primary identity of the key to the currently selected identity by clicking **„Set as Primary Identity...“**. The selected identity will be the primary identity from there on.

7.10.4 Public Key

On this page possibilities of how to distribute your public key have been placed at your disposal.

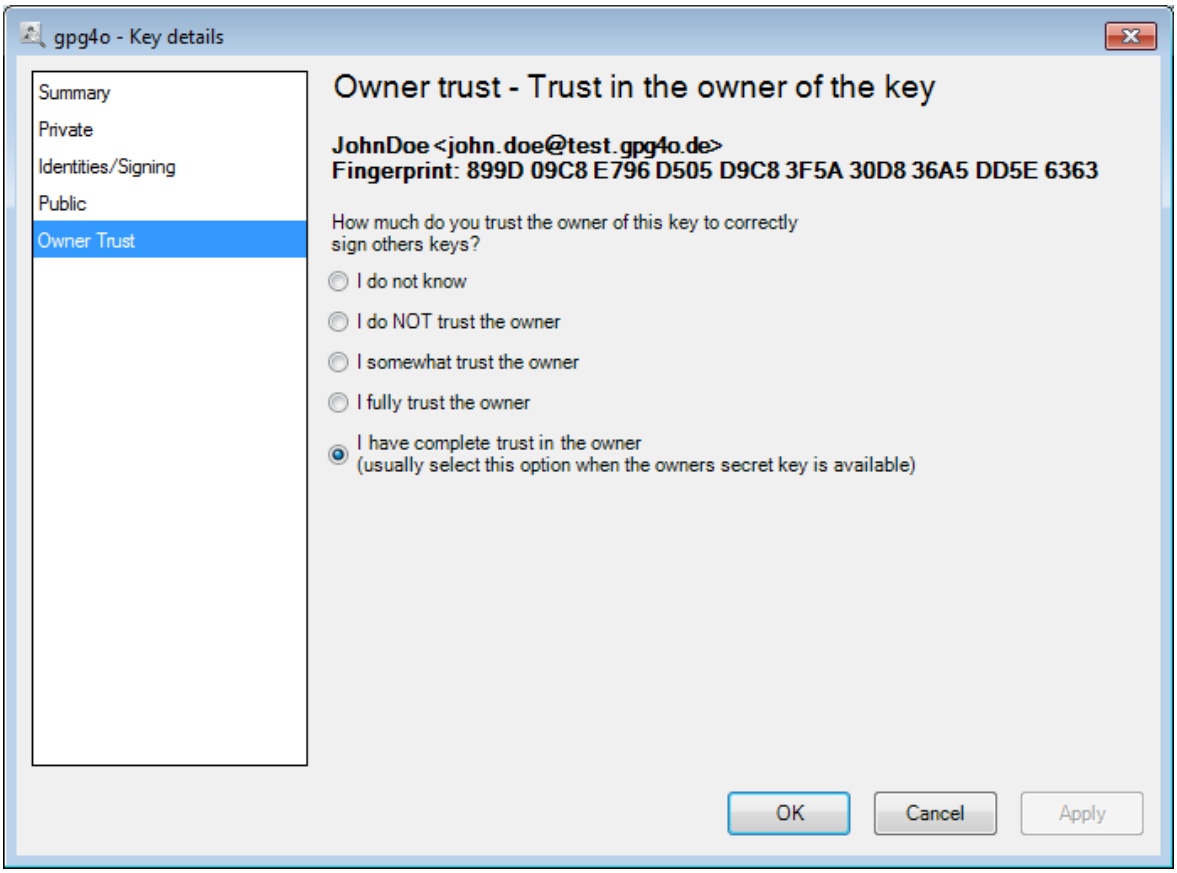


You can send your public key as an attachment to a new email or upload it to a keyserver from where it can be imported by your contact partners. Moreover, you have the possibility of exporting the public key as a file on your computer or a removable medium such as a USB-stick.

Tip: All those functions are also directly available to you in the overview by pressing the right mouse button on a key.

7.10.5 Define Owner Trust

By means of the owner trust you can define how much you trust your contacts to sign foreign keys and to classify them to be true. This permits to determine the key validity of other keys on the basis of its signatures. If another key was signed by the issuer of the key the owner trust of whom you set here, this will have direct influence on the key validity of the other key. This principle is called **„Web of Trust“**. In this connection also consider paragraph 7.10.1.



There are several selection possibilities at your disposal in order to define the trust in this contact. You should however only choose the option **„I have complete trust in the owner“** for own keys as this option will have another influence on the key validity as it is not intended for foreign keys.

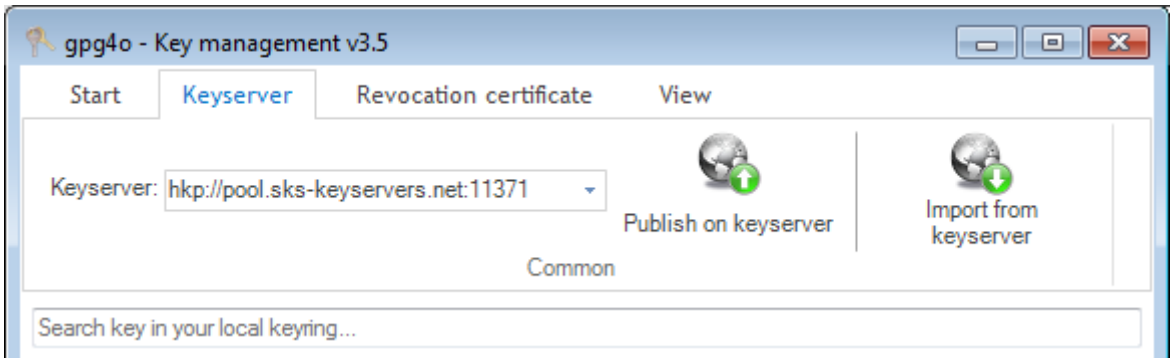
The level of trust indicated by you remains a secret of **GnuPG** and will, with the exception of the integrated backup function, never be exported or transmitted to anyone else.

Tip: You can also modify the owner trust directly by clicking the right mouse button on a key in the overview.

7.11 Utilization of Keyservers

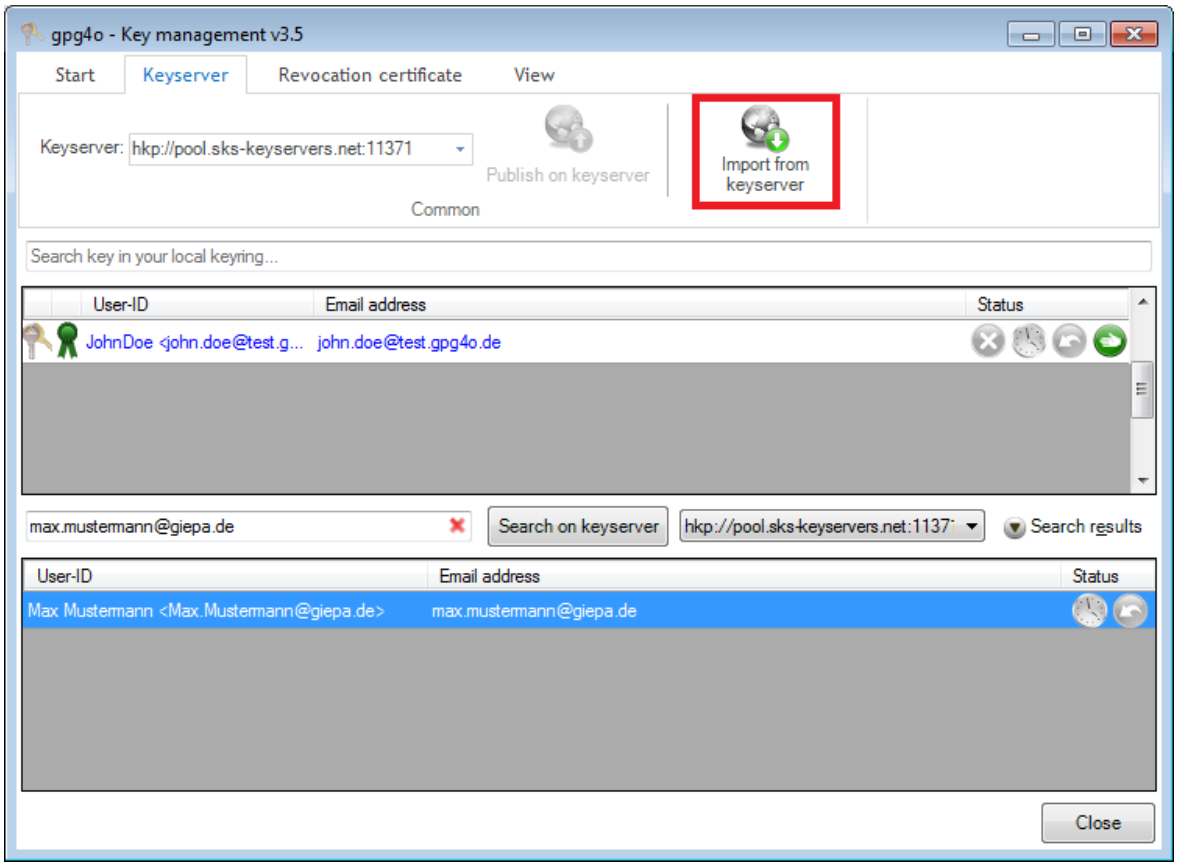
In addition to the possibilities to send keys per email, described in the paragraphs 6.1 and 6.2 you can also upload your public key on a keyserver in the Internet and from there also import public keys of your communication partners.

For this purpose go back to the overview of the key management and select your key. Change to the tab **„Keyserver“** in the menu ribbon and select the keyserver on which you want to upload your key.



Click the button **„Publish on keyserver“** then in order to upload the currently selected key(s). Now you only have to inform your communication partner of the selected keyserver so that he will be able to import your public key from there.

For importing a key from a keyserver you can enter your communication partner's name or key-ID in the search field in the lower section of the key management.



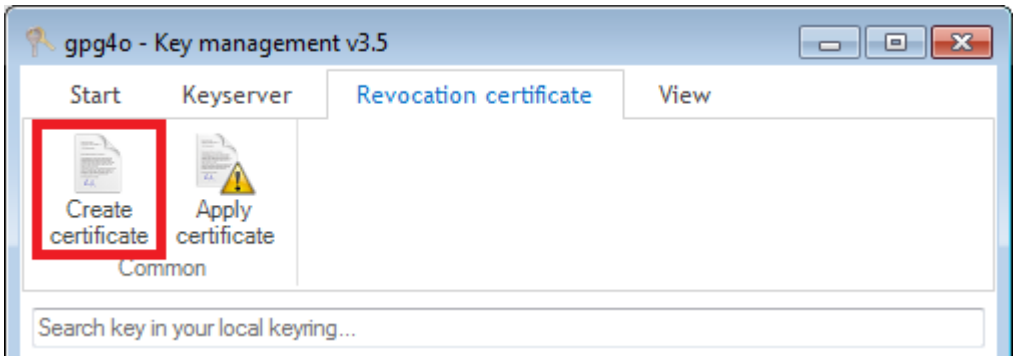
If the searched key is found you can select it and import it via the button **„Import from keyserver“**.

Tip: You can also import the key via a click on the right mouse button on the key which has been found or by holding the pressed left mouse button and drawing the key into the above list.

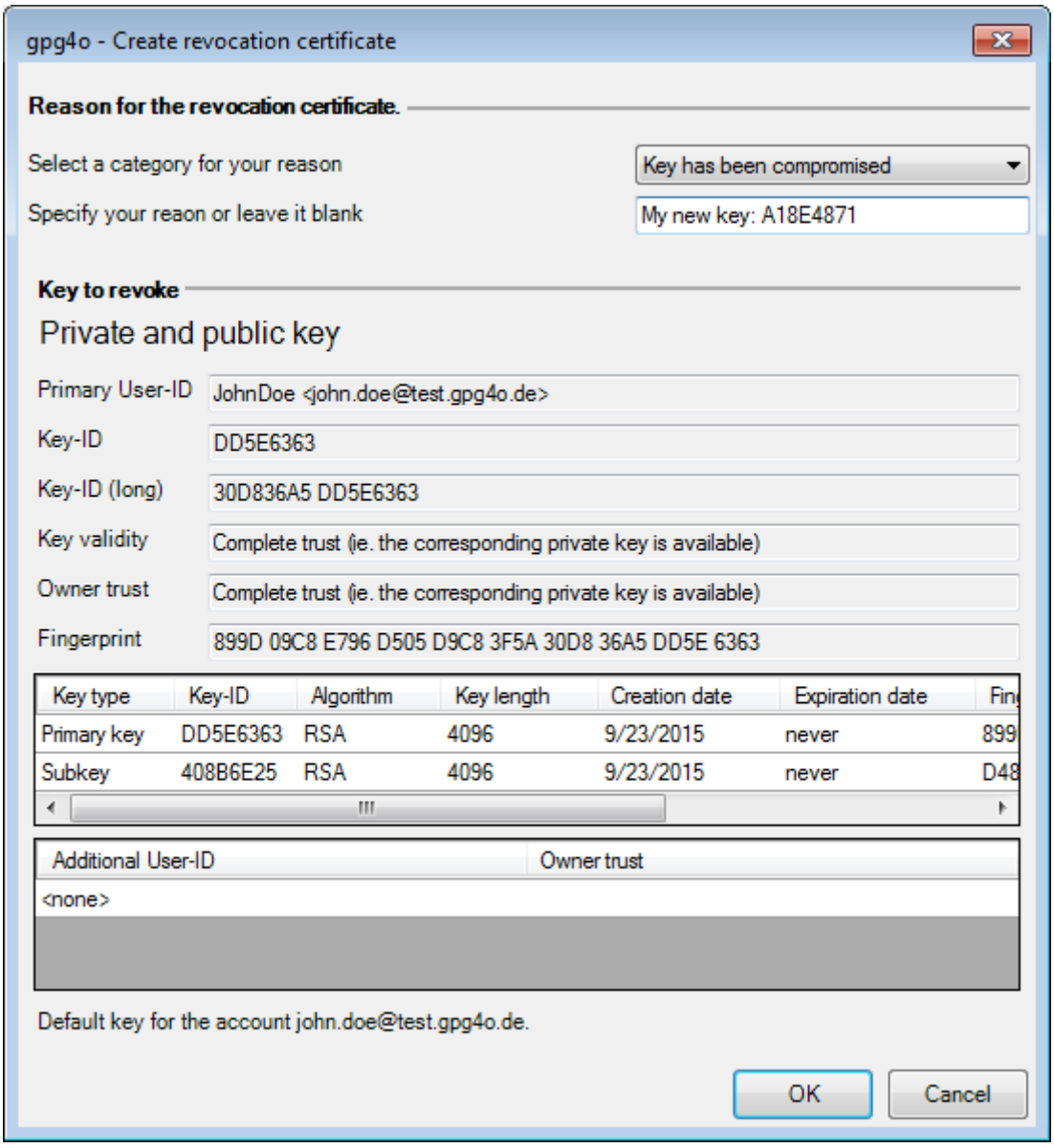
7.12 Generating Revocation Certificate

With a revocation certificate a key can be permanently and irrevocably declared invalid. With a public key declared invalid your communication partners can no longer write encrypted emails to you. This makes sense for example for the case that another person has taken possession of your private key and, thus, it cannot be secured any longer that emails signed with it have actually been generated by you.

For generating a revocation certificate please choose the corresponding key in the overview of the key management. Then select the button **„Generate revocation certificate“** via the menu ribbon in the tab **„Revocation certificate“**.



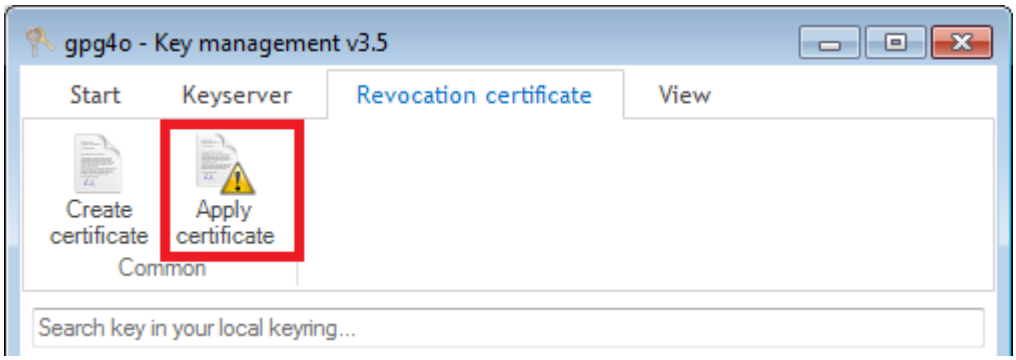
You will be asked for the reason why you want to generate a revocation certificate and can furthermore write a comment on it specifying the reason or furnishing additional information. This can be for example the key-ID of the new key which your contact partners shall utilize afterwards.



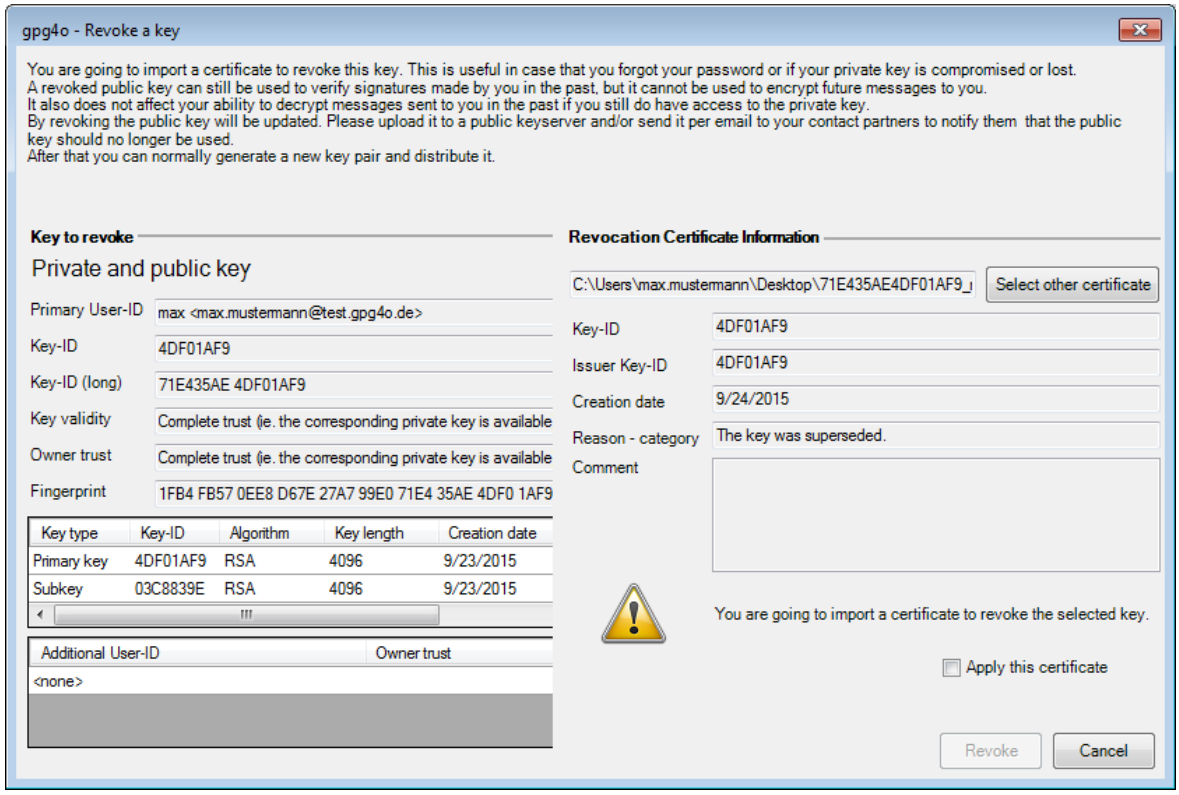
After having entered the reason click **„OK“** and indicate the folder where the revocation certificate shall be saved.

7.13 Applying Revocation Certificate

For the revocation of a key select it first and then go to **„Apply revocation certificate“** in the tab **„Revocation certificate“** in the menu ribbon of the key management.



Select the revocation certificate in the appearing file selection dialog and afterwards click **„Open“**.



First, check the information of the revocation certificate. If you are sure that you want to apply the revocation certificate place a checkmark with **„Apply this certificate“** and click **„Revoke“** then.

Attention: By revoking the key is made permanently unusable! In addition, the public key is updated and must therefore be distributed to your communication partners. If you have published the key on a keyserver too, you will have to upload the updated key again.

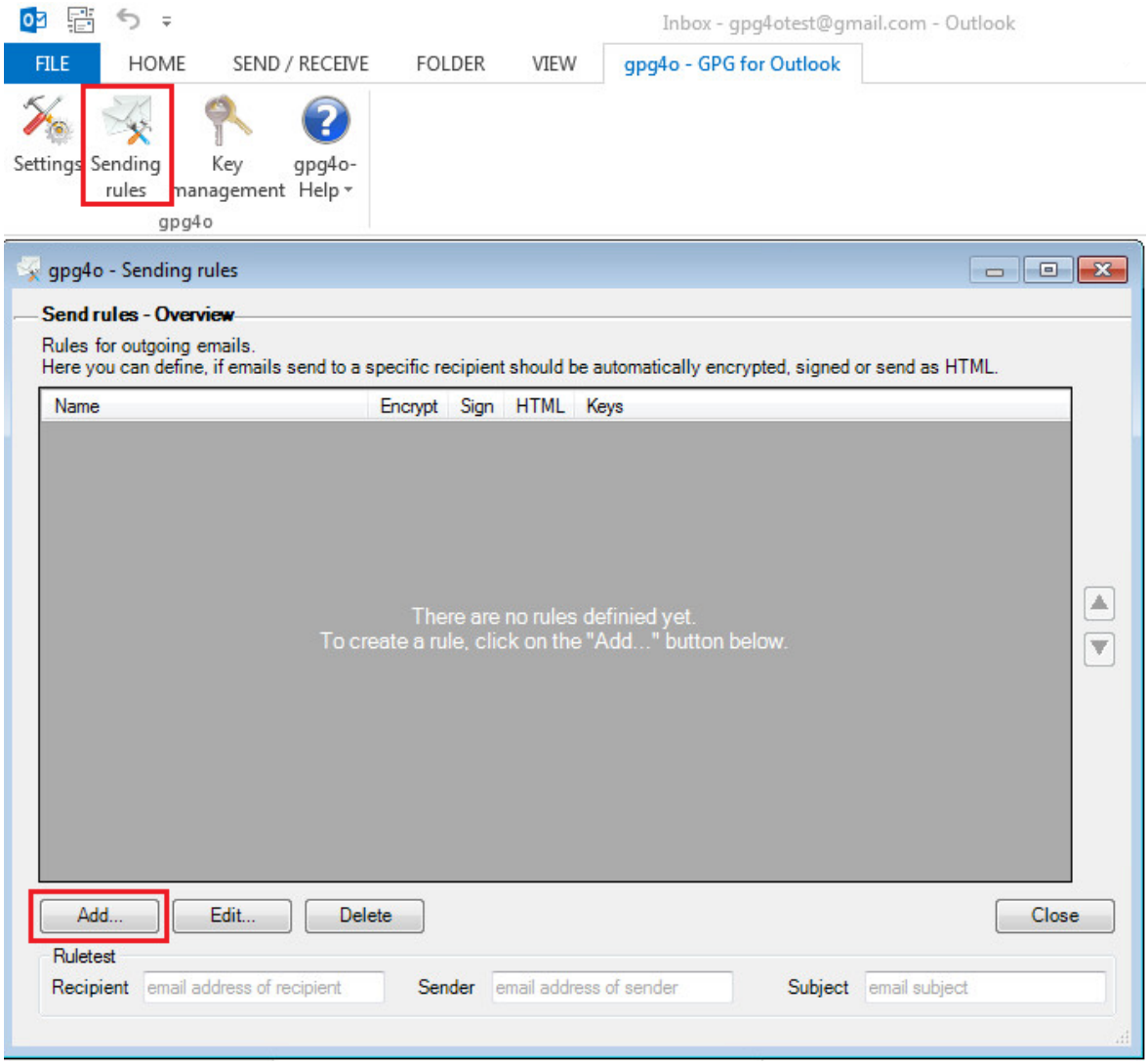
8 Sending Rules

In order to prevent you from having to manually select the settings for encrypting and signing for each of your emails, sending rules have been provided in **gpg4o** performing this task for you.

8.1 Management of Sending Rules

In the overview of the sending rules you have the possibility of sorting and testing your existing rules without any influence on the rule evaluation.

For that click the item **„Sending rules“** in the menu ribbon **„gpg4o - GPG for Outlook“**.

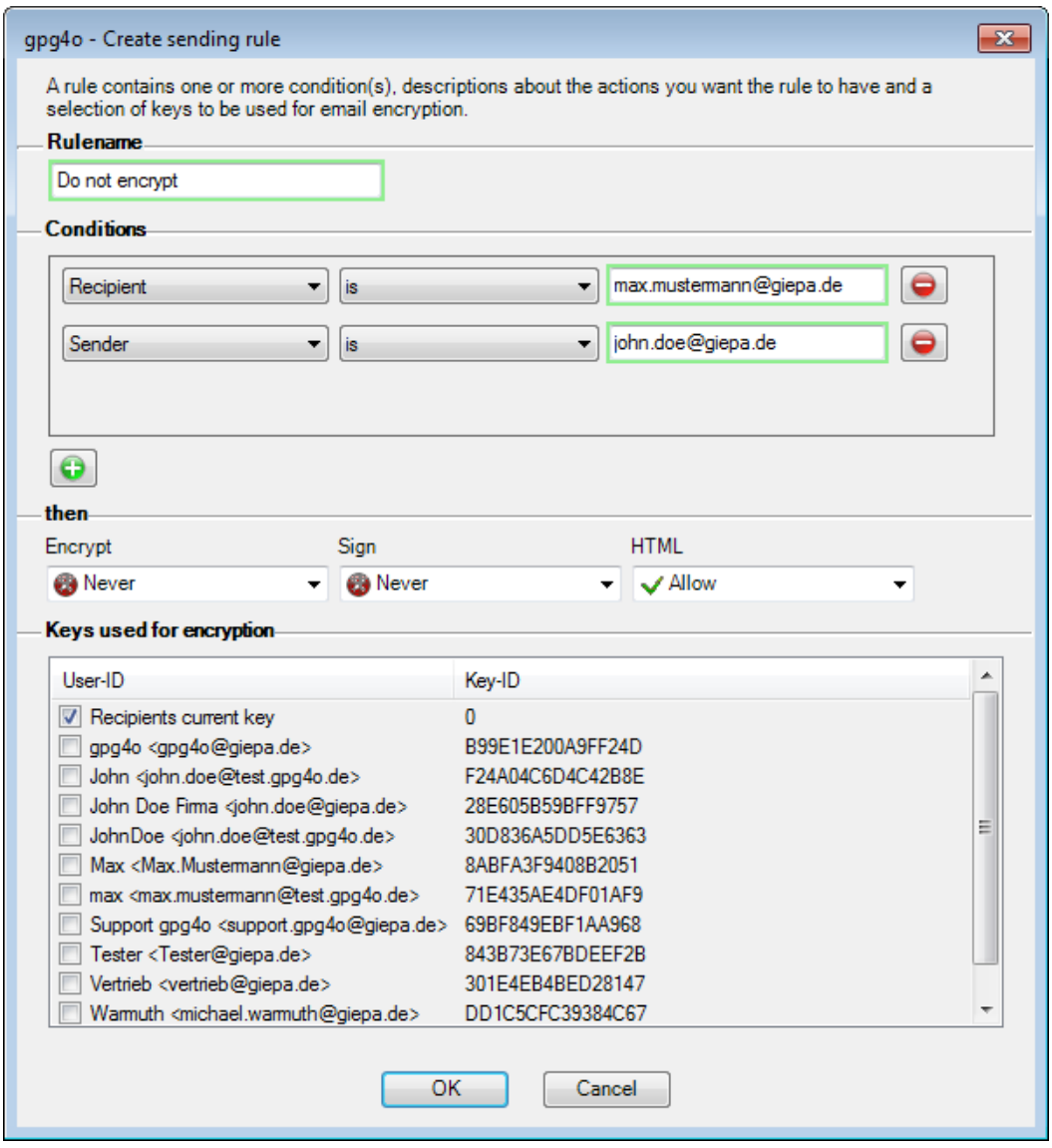


*For generating a new rule click the button **„Add...“** in the overview.*

In the field **„Rulename“** you enter an expressive name for this new rule. Having done

that, complete the conditions. When working out the conditions take care to make them as specifically as possible in order to avoid later conflicts.

Afterwards, you select the encrypting options to be utilized and the recipient's public keys. The keys will be utilized later for encrypting when sending the email if the rule is applied. If you want **gpg4o** to select the appropriate key for you, you leave the selection with **„Recipient's current key"**. Otherwise you select those keys here which shall be utilized for encrypting the email.



8.2 Rule Evaluation

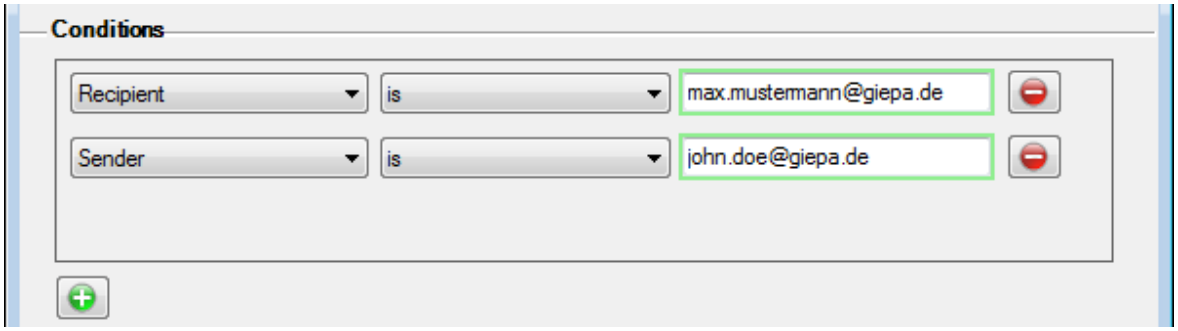
In order to apply a rule when sending an email **all** preconditions indicated in the domain **„Conditions"** have to be fulfilled.

When creating a new email all your rules are browsed and all matching rules are selected.

This selection is based exclusively on the conditions of the individual rules and not on the classification in the rules list.

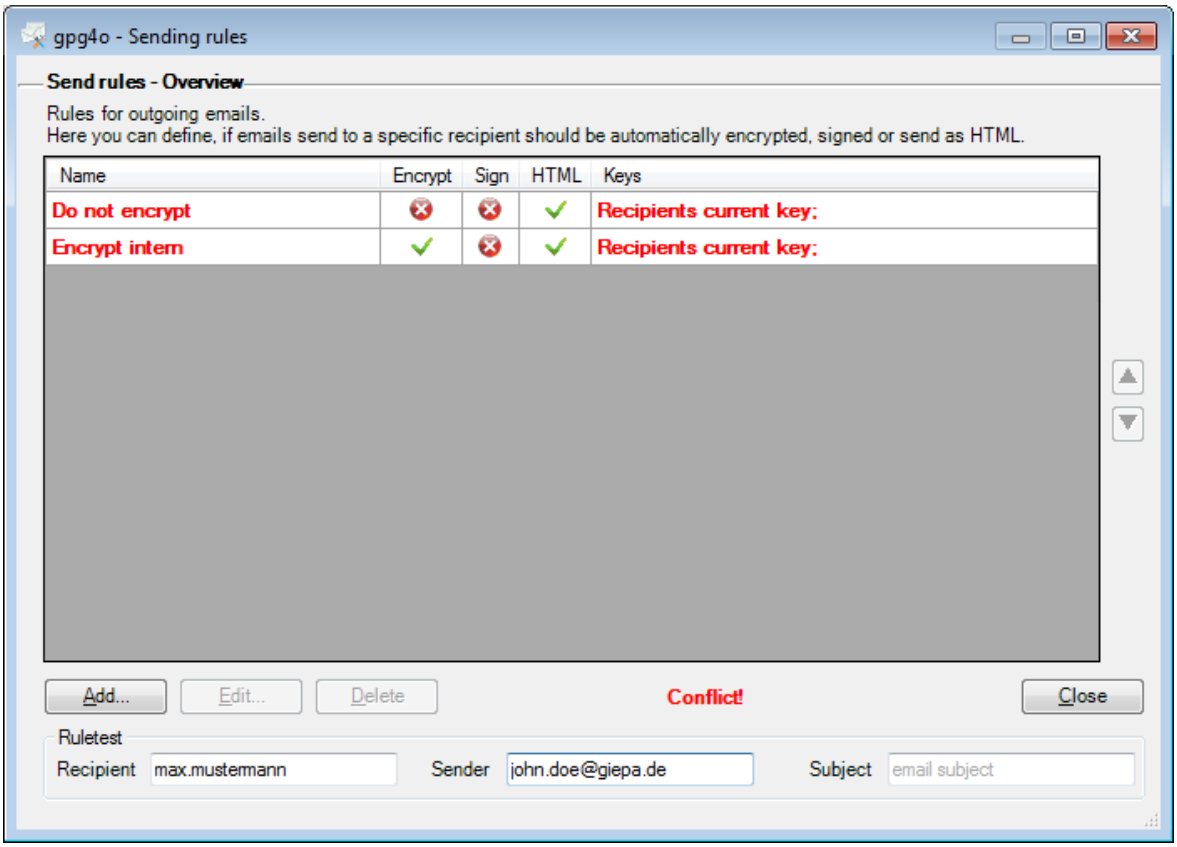
The following example shows two rules:

Rule **„Do not encrypt“** contains two conditions:



Rule **„Encrypt intern“** contains one condition:

If you write an email to **max.mustermann@giepa.de** now and if you select **john.doe@giepa.de** as sender, both of your rules will apply. Thus, you will come into conflict as the settings for encrypting within the rules are different.



In order to avoid this conflict in the future you can add further conditions to the rule **„Encrypt intern“**:

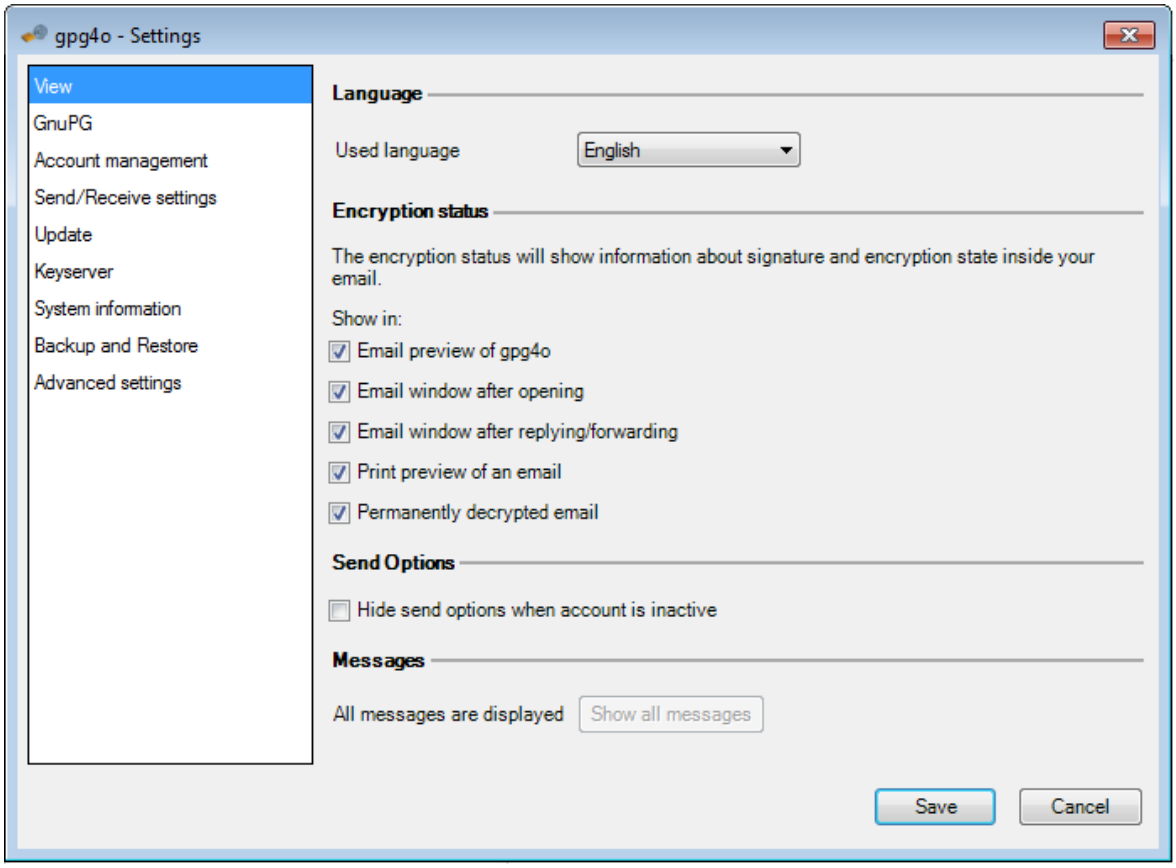
Recipient	is not	**max.mustermann@giepa.de**
Sender	is not	**john.doe@giepa.de**

9 Settings

With the settings you can adjust important options of **gpg4o**. Modifications of the options, even if you switch between menu points, only become effective after saving.

9.1 View

On this page the general configuration settings are displayed permitting to adapt the aspect of **gpg4o** and the integration into Microsoft Outlook® .



9.1.1 Language

The language may be adjusted between German and English. Please mind that when modifying the language the settings have to be closed and opened again.

9.1.2 Encryption Status

Here, you may select in which areas of **gpg4o** the information with regard to decryption and signature shall be displayed to you within an email. By default the display is only shown in the normal email preview.

9.1.3 Send Options

If this configuration setting is active the ribbon with the send options will be hidden when generating an email and the selected sending account has not been enabled for utilization with **gpg4o**.

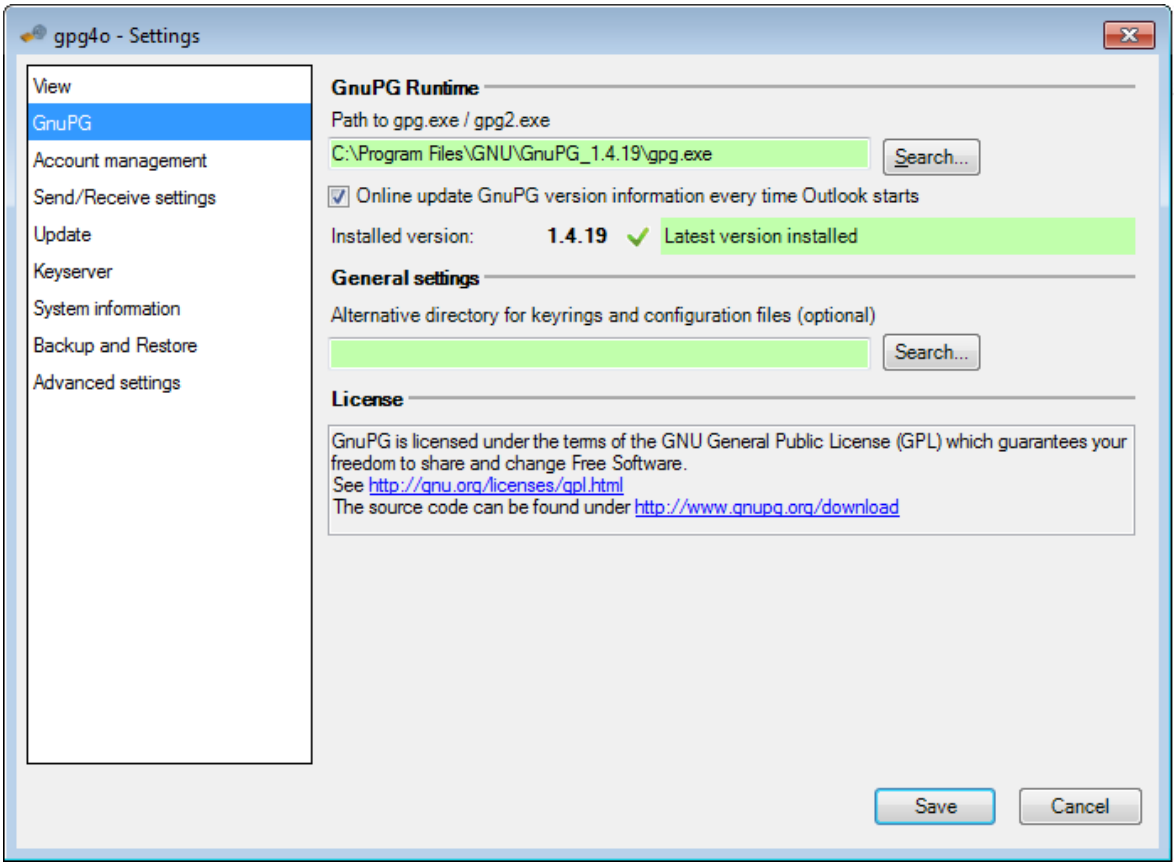
If the configuration setting is not active the send options will also be indicated in case of inactive accounts.

9.1.4 Messages

As the user, you can decide whether or not you want to deactivate the repeating question so that it does not appear anymore. An example would be the messagebox which appears when a newer **GnuPG** version is found online within the start of Outlook. By confirming this through the button, you are activating all deactivated messages again.

9.2 GnuPG

On the page **GnuPG** the version and the path to the installed **GnuPG** are displayed.



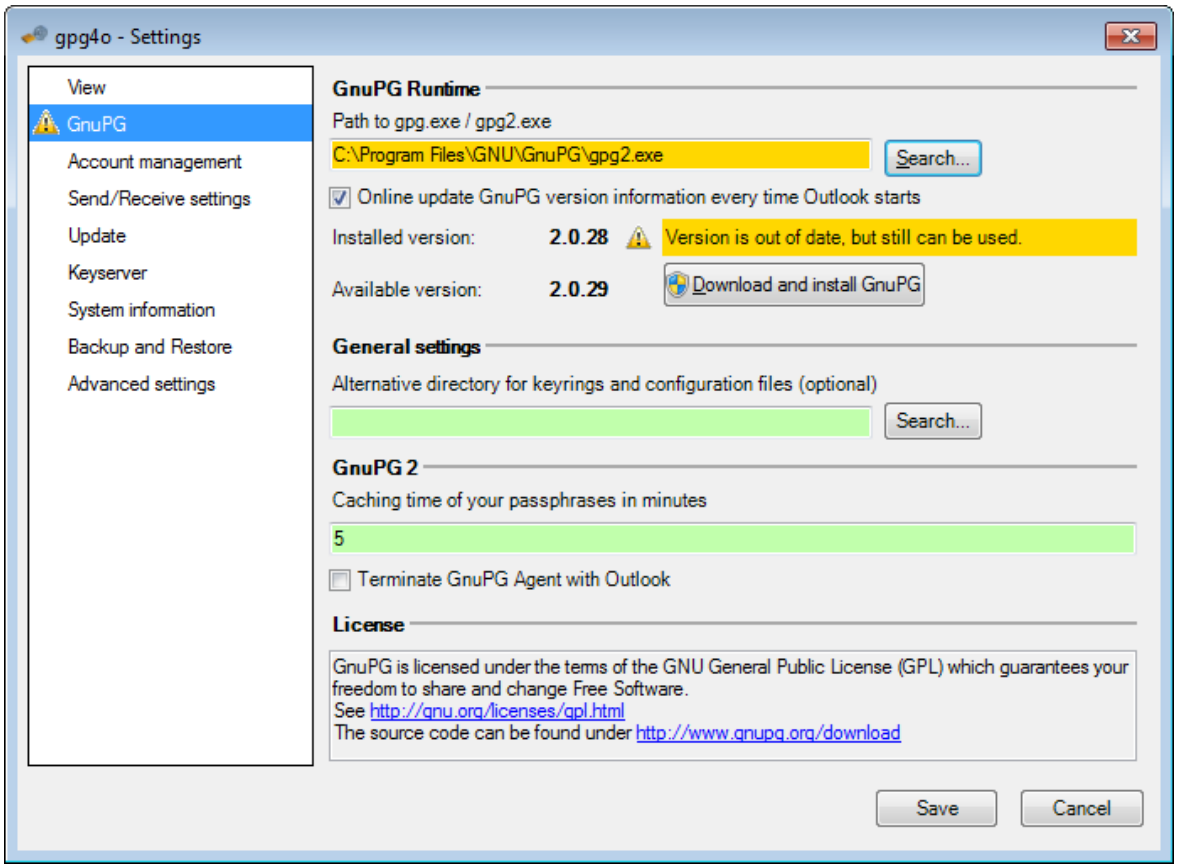
9.2.1 Path to gpg.exe/gpg2.exe

If necessary, you can also convert to other installations of **GnuPG** with the help of the button **„Search...“**.

If you have not yet installed **GnuPG** the button **„Download and Install“** will be shown to you below the version number with which you can download **GnuPG** from the Internet and install it. Here, the procedure is the same as with the installation by the configuration wizard.

Here, you will also find information with regard to the license of **GnuPG** and you have the possibility of obtaining further information by means of the links, if available.

9.2.2 GnuPG Version Checking



gpg4o uses **GnuPG** to encrypt emails. This program is constantly being developed and receives regular updates and new features. To keep **GnuPG** up to date, please activate the option **„Online update GnuPG version information every time Outlook starts“**.

You receive a message when starting Outlook, when a new version of **GnuPG** is released. You can then decide whether or not you want to install this new version. Confirming the question with **„Yes“** will redirect you to the page **„GnuPG“** of the **gpg4o** settings. There you can click on the button **„Download and install GnuPG“** which will download and install the latest version.

9.2.3 GnuPG Directory

By default **GnuPG** saves its keyring in the application folder of your user profile. If you want to make use of another directory instead you can select an alternative directory here. This directory will then be utilized in the future instead of the default directory of **GnuPG**.

Hint: Already imported or generated keys will not be copied and will no longer be available in the new directory. In the old directory, however, they will still be existent. In order to be able to access these keys you have to export them before and import them again after having changed to an alternative directory (see paragraph 7).

9.2.4 GnuPG Agent

Since **GnuPG** 2.x the **GnuPG Agent** is applied in order to buffer the passphrase. The agent is automatically started as soon as a **GnuPG** action in **gpg4o** is made. However, when closing Microsoft Outlook® the **GnuPG** agent is not terminated by default. Thus, buffered passphrases are not reset which might produce a security risk.

If you enable this option the **GnuPG Agent** will be terminated automatically with Microsoft Outlook® thus removing preliminarily entered passphrases from the memory.

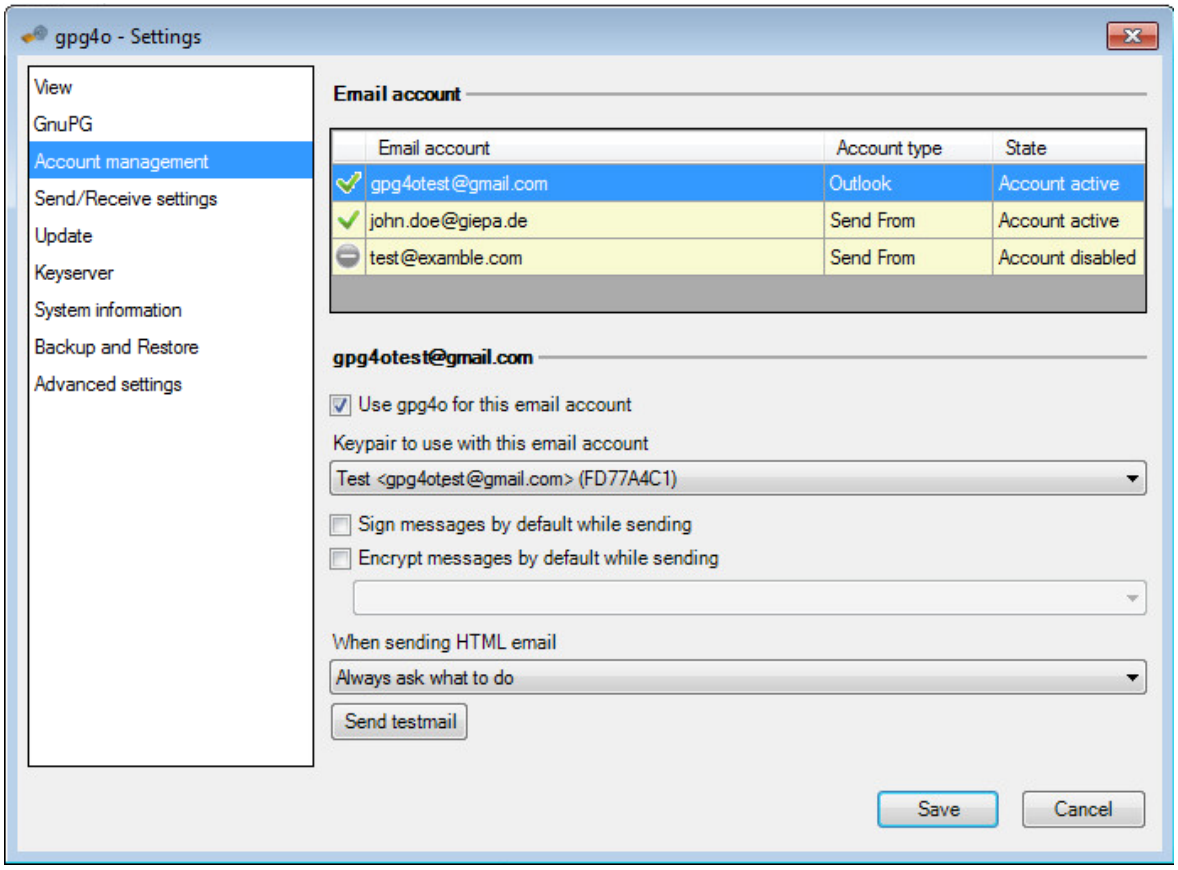
Hint: The starting of the **GnuPG Agent** may take some seconds. This can be noticed in particular if you select the first email for decrypting.

9.2.5 Buffering of the Passphrase

If you are using **GnuPG** 2.x you can determine here how long the passphrases you have entered shall be buffered. The minimum duration of how long the passphrases are buffered, is one minute.

9.3 Account Management

On this page the configuration of the individual email accounts is performed (usually one email address corresponds to an account in Microsoft Outlook®).



Under the name of the selected email account you will find the associated settings. Place the checkmark with **„Use gpg4o for this email account“** if you want to decrypt messages in this email account or if you want to send messages encrypted and/or signed.

Hint: If you do not want to encrypt or sign at all in an email account you should disable **gpg4o** for this account.

With the selection box **„Keypair to use with this email account“** you define which keypair shall be utilized for signing messages.

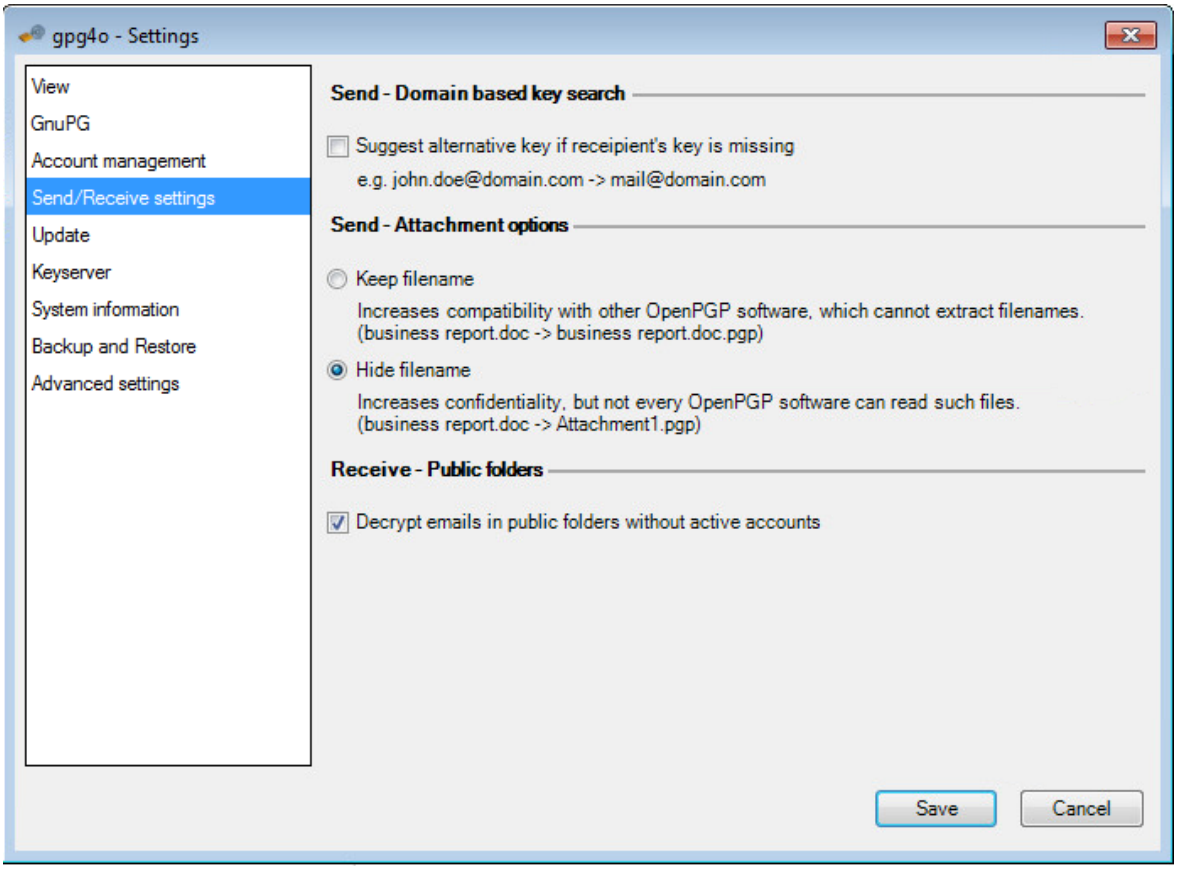
With the next two check boxes the default behavior of **gpg4o** with regard to the sending of emails is determined. If you choose messages to be encrypted by default you also have to define whether only the attachments or the entire message shall be encrypted.

If you regularly necessitate other configurations for certain situations you can set them with the help of the sending rules (see paragraph 8).

The function of the selection box **„When sending HTML email“** is to determine whether when sending emails in HTML format a default demand has to be made, whether the HTML format may be utilized or whether it shall be converted into the Plain-Text format before sending.

You can send a testmail for the selected account. You can verify with the received testmail whether encrypting and decrypting work correctly with your settings.

9.4 Settings for Sending and Receiving

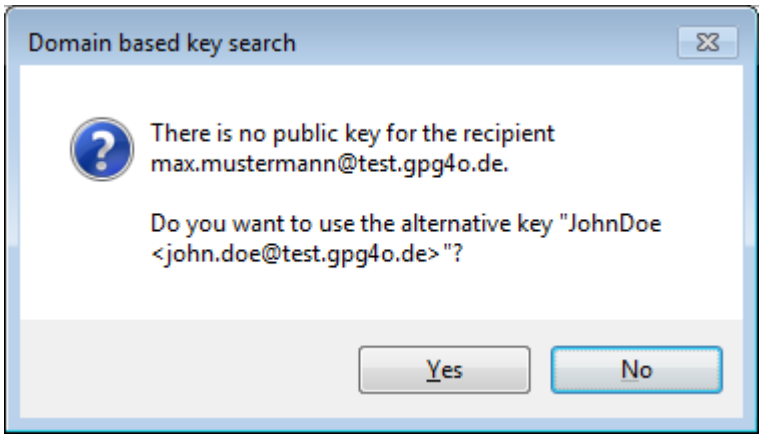


9.4.1 Domain Based Key Search

You can enable the **„Domain based key search“** if you do not want to search for a corresponding key for every missing key or if you own a global key for a company. Thus, a possible suitable key from the recipient's domain will be automatically proposed to you from your key list in case of a missing key.

In order to enable the domain based key search place a checkmark with **„Suggest alternative key if recipient's key is missing“**. **gpg4o** will do the rest for you.

If you write an email to **„Max.Mustermann@giepa.de“** but if you do not own a key for that recipient **gpg4o** can now offer you an alternative key from the corresponding domain.



If you refuse that key you may perform - as normal - the manual selection for encrypting your email.

9.4.2 Attachment Send Options

Many **OpenPGP**-applications do not only encrypt the email and the attachments but also the file names of the attachments. **gpg4o** masters this technique and uses it as standard. However, not every **OpenPGP**-application is compatible with this technique. Therefore, you should activate the option **„Keep filename“** if a recipient cannot decrypt the file names.

9.4.3 Public Folder

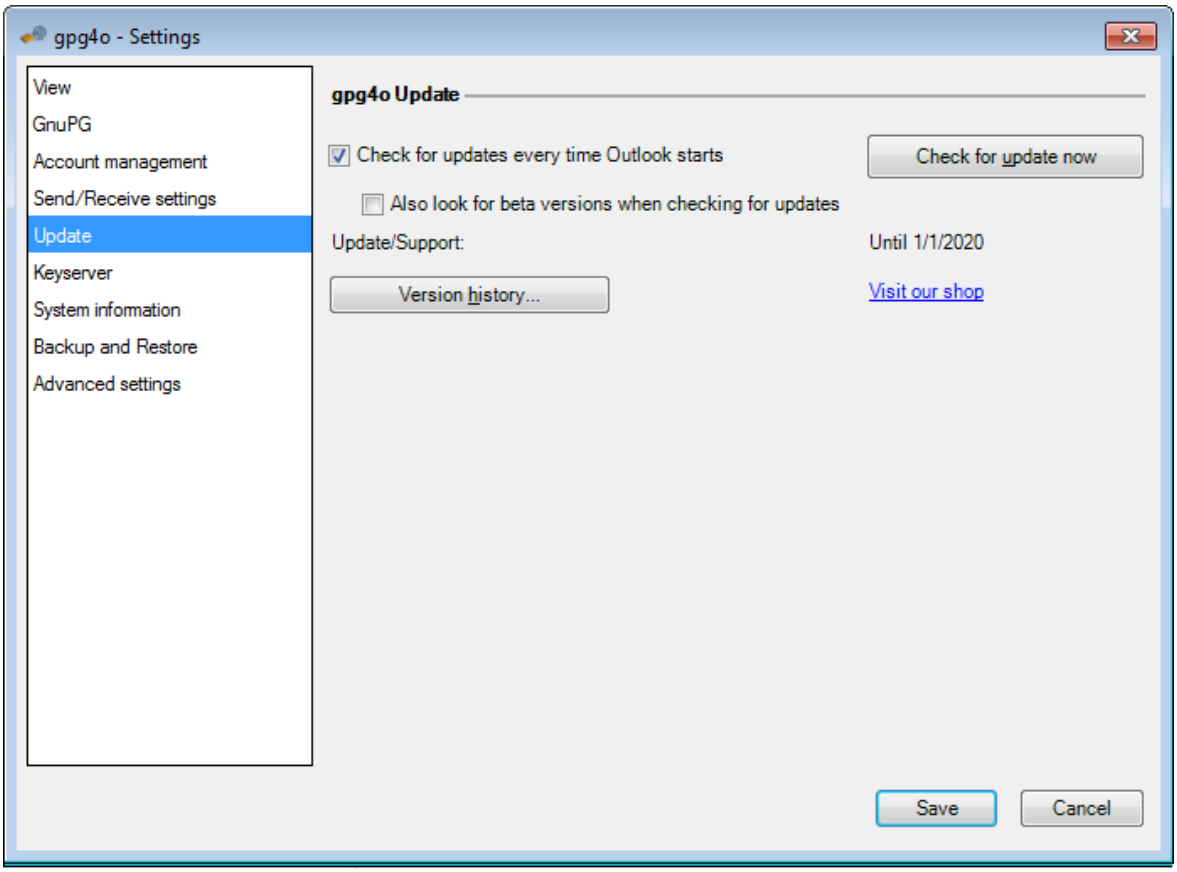
As standard you can only decrypt those emails which can be found in the folder of an account enabled in **gpg4o**.

With this option you instruct **gpg4o** to decrypt emails in public folders irrespective of your active accounts. The only precondition is that you own the private key of the recipient to whom the email was sent. You can now let you show your emails as usual.

Please mind that this option is only utilized in public folders. For decrypting emails in other folders the corresponding account has to be enabled (see paragraph 9.3).

9.5 Update

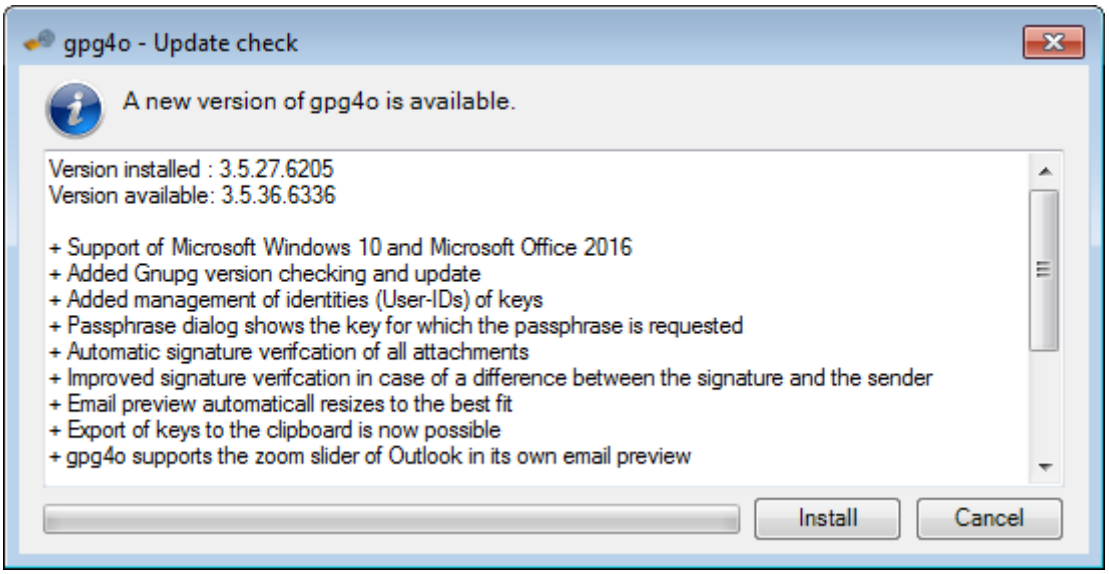
The developers of **gpg4o** regularly extend the software, improve its usability and add new features (customers' desires).



On this page you can perform a manual check for updates by clicking the button **„Check for update now“**. If this verification shall be performed regularly place the checkmark with **„Check for updates every time Outlook starts“**. By this, every time you start Microsoft Outlook® a newer version of **gpg4o** is searched and this version is offered to you for installation.

You have an option to install an early release version of the latest **gpg4o**, by activating **„Also look for beta versions when checking for updates“**. Through this, you can see the improvements and new features of the upcoming version. You can also actively participate in the development of **gpg4o** by letting us know about the errors. Beta versions are usually released a few weeks before a new version of **gpg4o** is published.

Hint: Please note that a beta version can contain errors. You should not use these versions in a productive environment.



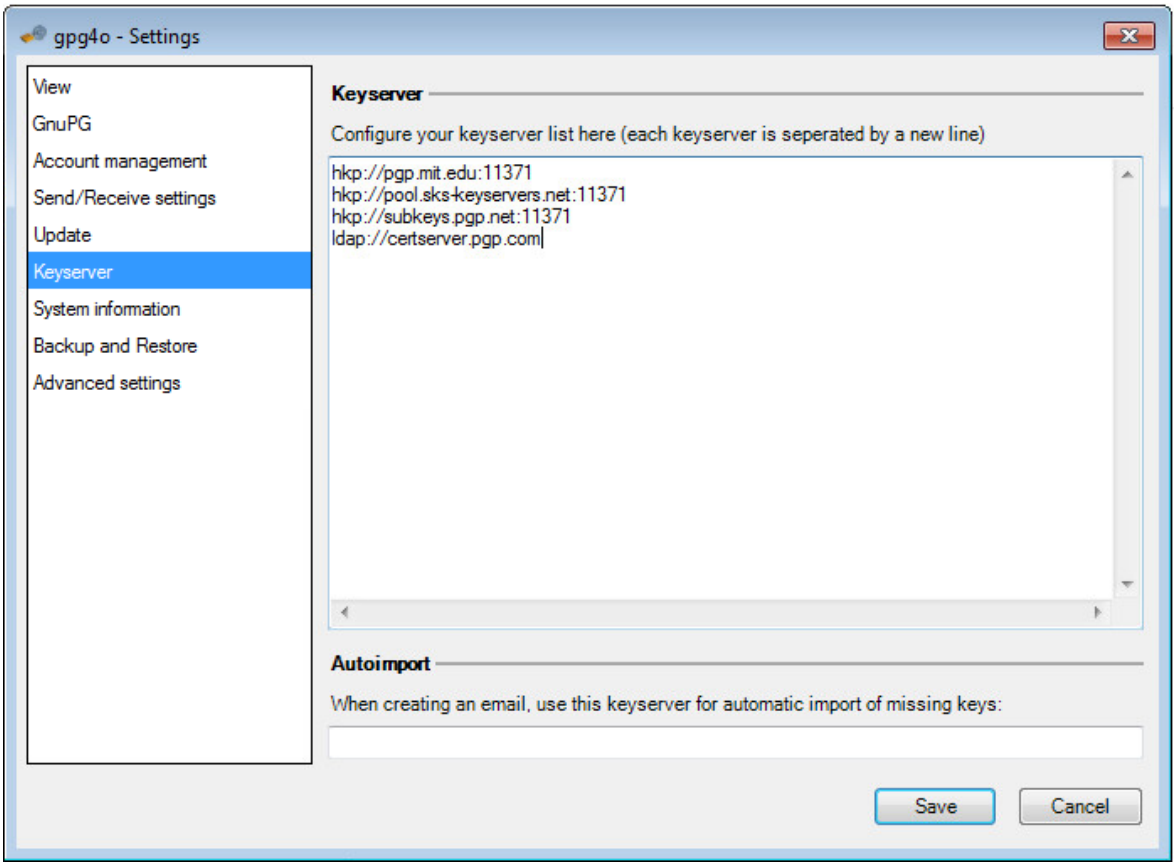
The updates are installed in the background and do not require any confirmations on your part. When the installation is finished you should make a new start of Outlook® so that the modifications become effective.

With the link **„Visit our Shop“** you can purchase a license of **gpg4o** or an extension of the product maintenance of **gpg4o**.

In the **„Version history...“** the individual releases and their improvements of **gpg4o** can be looked up.

9.6 Keyserver

On the page **„Keyserver“** you have the possibility of displaying and editing the keyservers utilized by **gpg4o**.



9.6.1 Keyserver

In order to add a new keyserver enter its address as a new line in the text field.

Hint: Keep in mind that the address of the keyservers will not be checked with regard to validity and that a wrong server cannot be reached.

In order to remove a keyserver, remove its entry in the text field. Thus, this keyserver will not be utilized in **gpg4o** anymore.

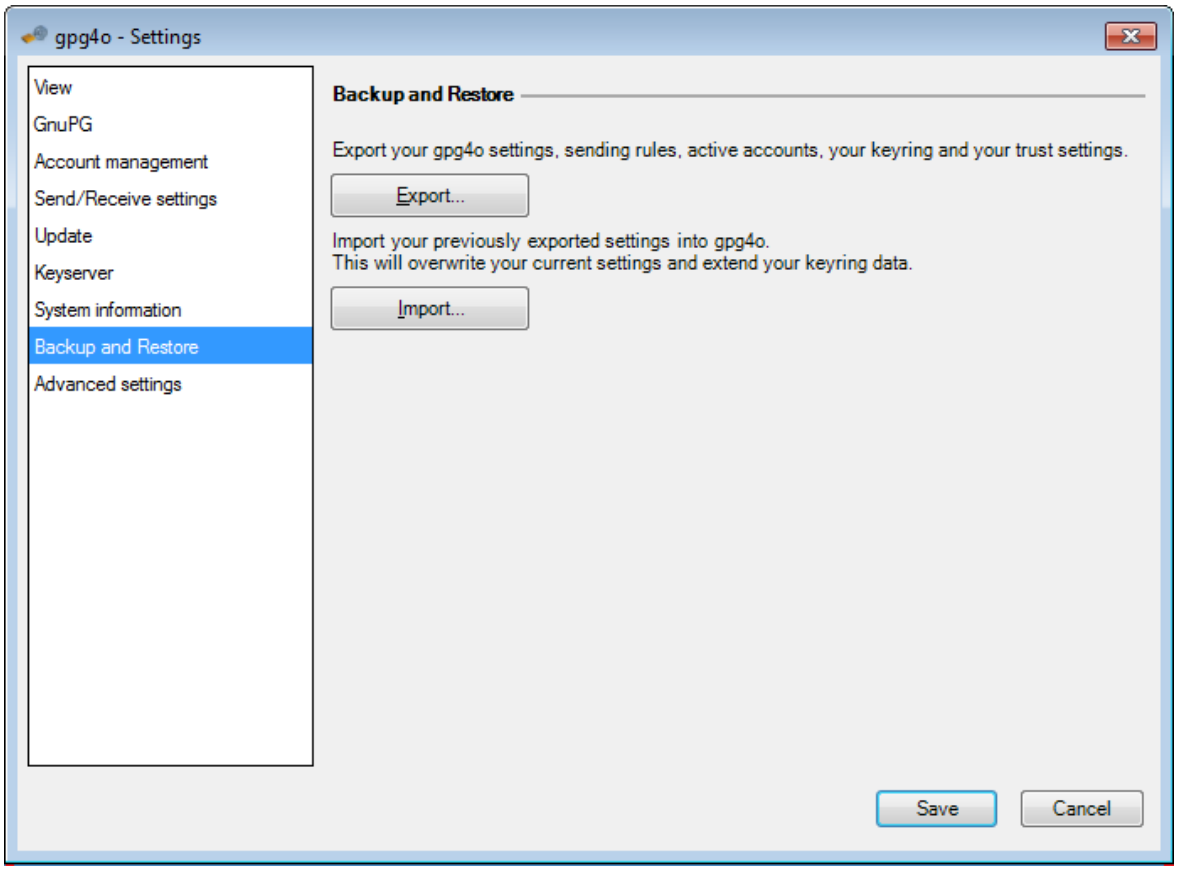
9.6.2 Autoimport

Here, you may enter a keyserver from which keys will be automatically imported into the local keyring while you generate an email. This is reasonable for example if you yourself work with a private keyserver and only upload valid keys there.

The server indicated in this field need not necessarily be entered in the list of all keyservers above in order to permit its use.

9.7 Backup

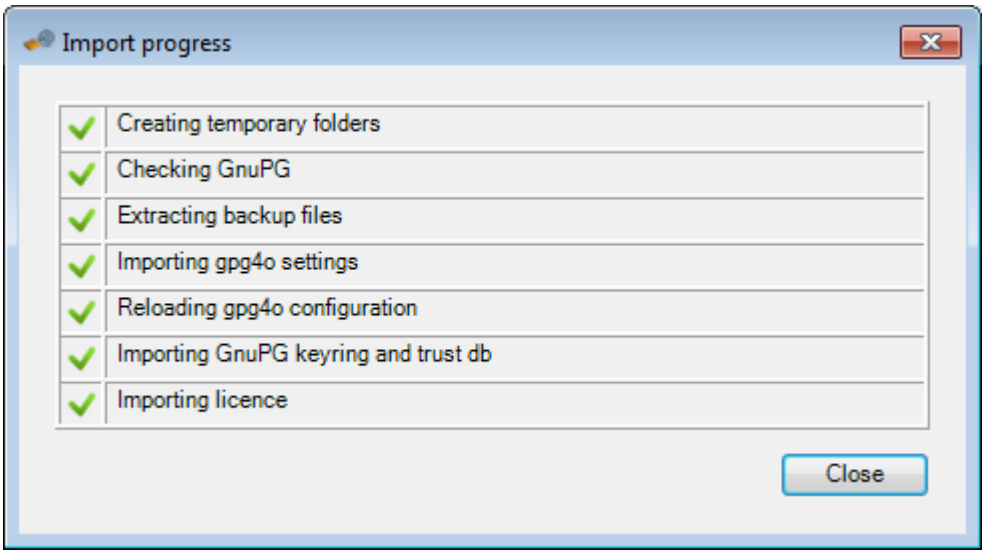
On this page you can import a saved backup or generate a backup, respectively. Above all, a backup protects you from the loss of your keys in case of hardware failures.



Via the button **„Export“** you generate a new backup. It comprises the following data:

- All the keys, public keys as well as keypairs
- The trust settings of the keys
- The complete configuration of **gpg4o** including all account-settings
- All defined sending rules
- The **gpg4o** license file

With the button **„Import“** you reload your preliminarily exported settings of **gpg4o** and, thus, overwrite your current ones. Your keyring will be extended by the newly added keys and those keys which were deleted since the last export, will be included again.



Tip: A backup may also be utilized in order to move **gpg4o** to another computer.

Attention: Only save the backup on your own physical data storage medium. You should **never** upload the backup into the cloud.

9.8 System Information

In the system information you can find details regarding the product **gpg4o**, the license, the operating system and **GnuPG**. There you can see, among others, the installation paths of the individual products.

9.9 Extended Settings

On this page you will find settings which do not necessitate any modifications in the normal operation or which do not require a better knowledge of the **OpenPGP**-Encryption. We kindly ask you not to modify anything here, if you do not know about the consequences of these modifications.

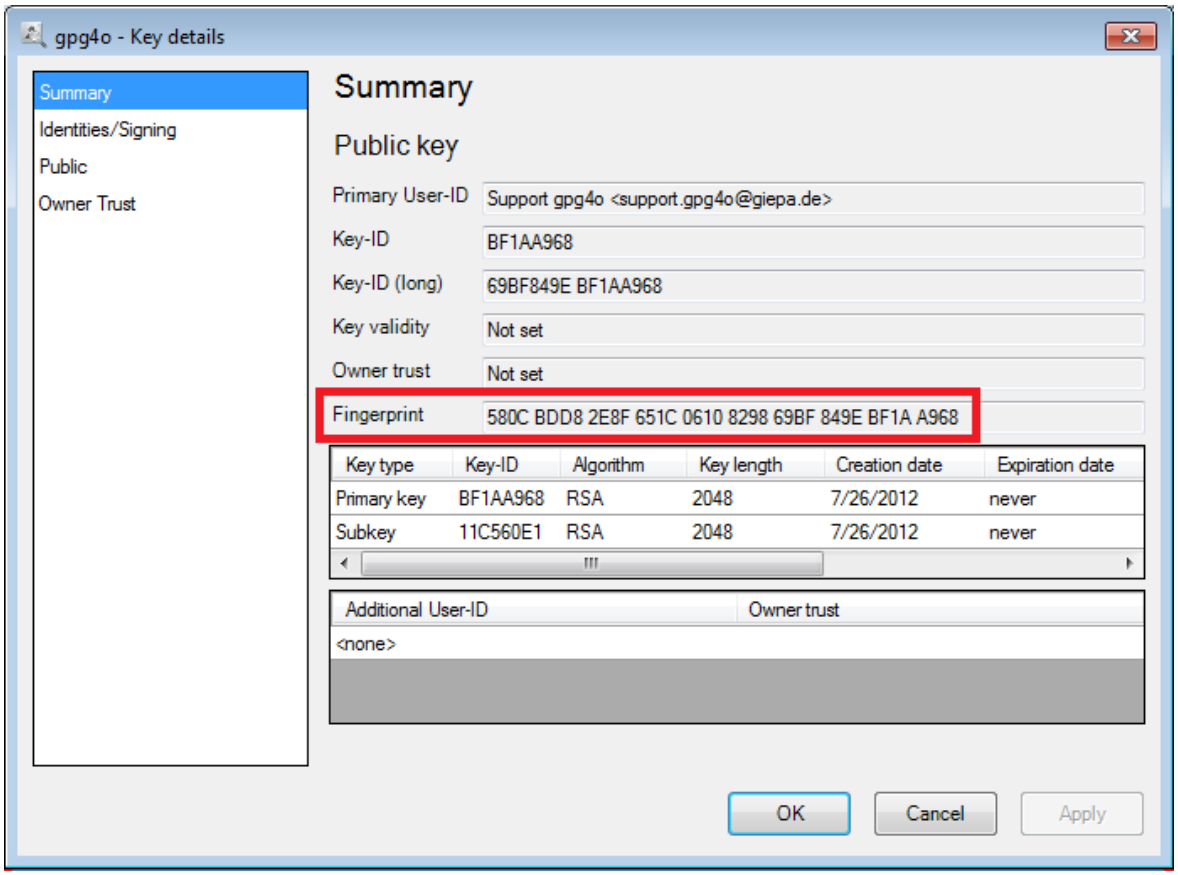
9.9.1 Always treat all keys as valid

It is true that deactivating this option will improve safety, however, it will also increase complexity and will require a considerable additional effort regarding the key management. If you disable this option you will only be able to encrypt emails to be sent to those recipients whose key you have signed or whose key has been recognized as valid by the **„Web of Trust“**.

Example:

Here explain how you can check the authenticity of a key and make it valid. In this case we are checking the authenticity of the **gpg4o** Support address of Giegerich & Partner and making it valid.

Please open the key management and search for the key **„Support gpg4o <support.gpg4o@giepa.de>“**. Select the key and open the key details.



Please compare the fingerprint in the key details with the following fingerprint:

```
580C BDD8 2E8F 651C 0610 8298 69BF 849E BF1A A968
```

If the given fingerprint matches the fingerprint shown in the key details, then you can set the authenticity of the Support key of Giegerich & Partner. Afterwards you can use this key for safe communication.

To validate a key, please read the paragraph **„Identities/Signing“** (see paragraph 7.10.3).

Hint: You have to check and validate each and every key if you have deactivated thet switch **„Always treat all keys as valid“**, before you can use them.

9.9.2 Insert GnuPG and gpg4o information in outgoing emails

If you encrypt and/or sign an email with **gpg4o** the **GnuPG**-Version and the **gpg4o**-Version will be inserted in the **GnuPG** headlines if the option is active. As this has also been implemented like that for other **OpenPGP**-solutions this option is enabled as a standard. However, you may also disable it in order to improve your safety. If one of your recipients has problems with decrypting and/or displaying the email he will not be able to read with which software

the email was encrypted.

9.9.3 Advanced signature check activation

By default this option is disabled. If you select a PGP/MIME signed email you can activate the advanced signature check. This option will kept active for all further PGP/MIME signed emails.

10 Miscellaneous

10.1 What Is to Be Done in Case of Errors?

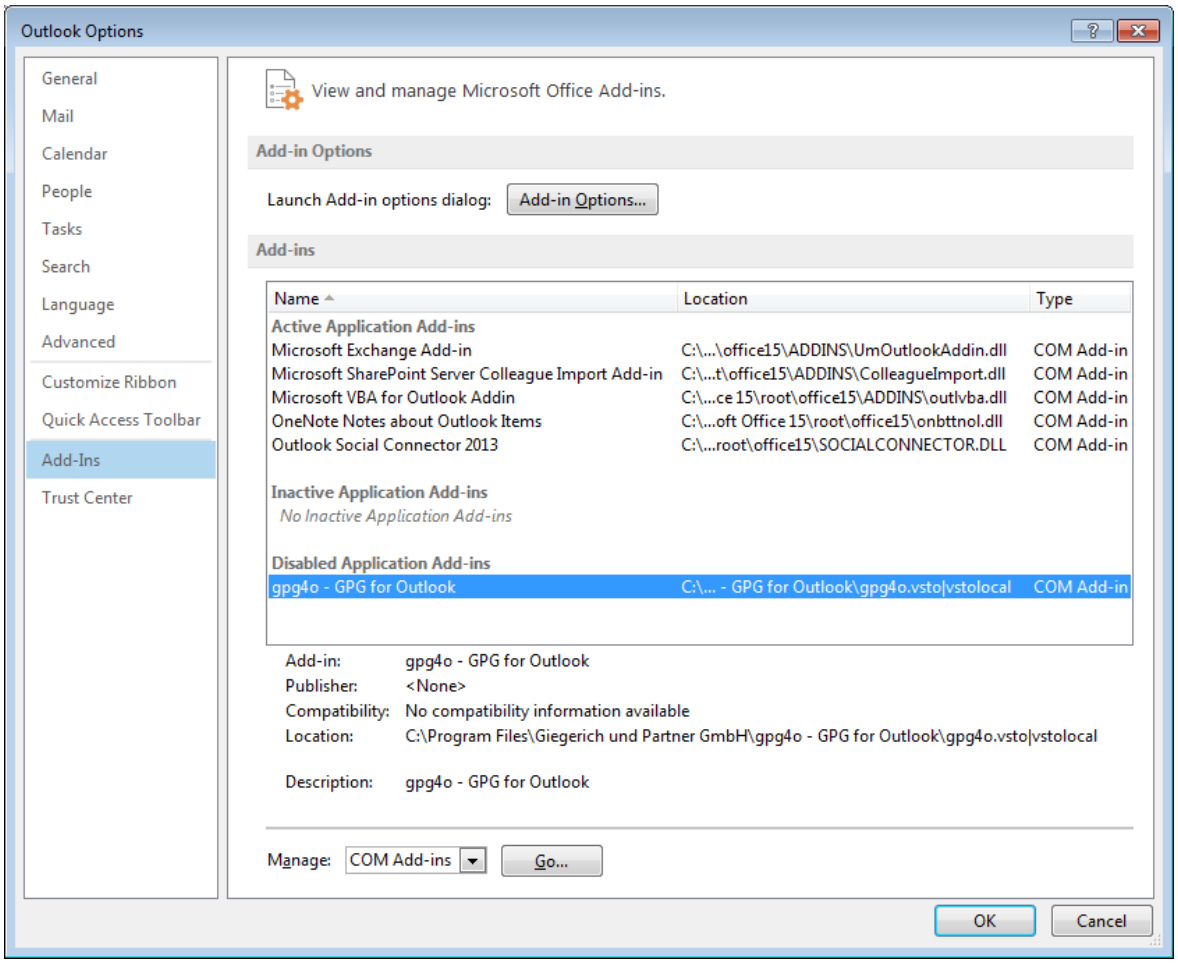
We kindly ask you to help us disclose and correct errors.

In order to be able to rapidly correct appearing errors we need a maximum of details concerning the error occurred. We kindly ask you to send us the error reports as well as the log files via the corresponding email provided in **gpg4o**. (see paragraph 11.1)

If you have questions, critical remarks or suggestions for improvement we kindly ask you to submit them to us in the same way or to write to our **gpg4o & GnuPG Newsgroup** (see paragraph 11), for we are always receptive to listen to your problems.

10.2 gpg4o does not Start

If **gpg4o** is not visible anymore there are several possibilities of reactivating the add-in again. First of all, kindly open your Outlook options by clicking **„File“** in the menu ribbon and selecting the menu item **„Options“** there. In the following window click on the left side **„Add-Ins“**.



Now, search on the right side the entry **„gpg4o – GPG for Outlook“**. If **gpg4o** can be found under the item **„Disabled Application Add-ins“** you are asked to follow paragraph 10.2.1.

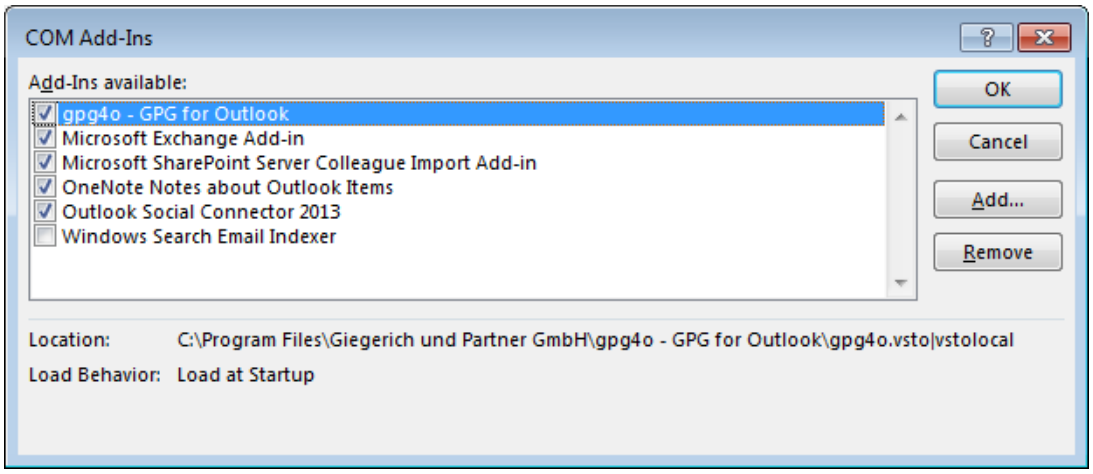
If **gpg4o** can be found under the item **„Inactive Application Add-ins“** please follow paragraph 10.2.2.

10.2.1 Disabled Application Add-ins

Select in the lower section next to the button **„Go“** the entry **„Disabled elements“** and afterwards click the button **„Go...“**. In the window opened then select the entry **„gpg4o – GPG for Outlook“** and click the button **„Enable“**. Having done that, close the window by clicking **„Close“**. After a moment **gpg4o** will be loaded again. Otherwise, it might be necessary to enable **gpg4o** subsequently via the procedure described in paragraph 10.2.2.

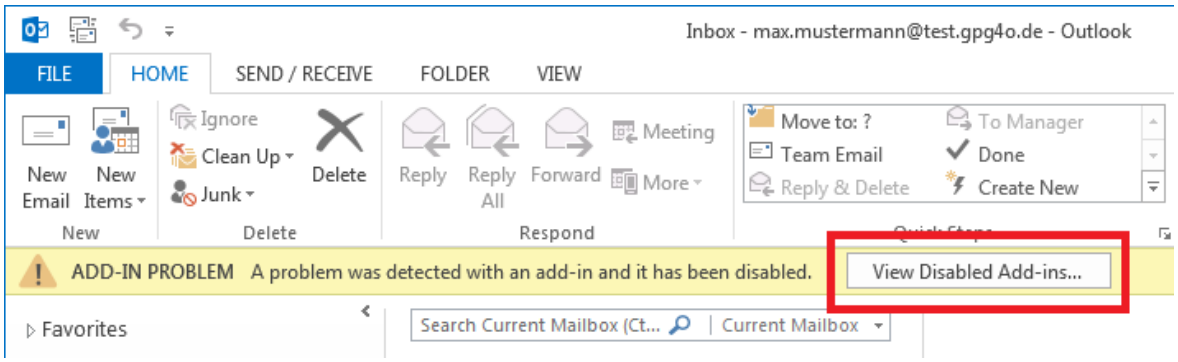
10.2.2 COM-Add-Ins

Select in the lower section next to the button **„Go...“** the entry **„COM-Add-Ins“** and click the button **„Go...“** then. In the window open now search the entry **„gpg4o – GPG for Outlook“** and place a checkmark in front of it. Afterwards, close the window by clicking **„OK“**. After a moment **gpg4o** should be reloaded. Otherwise, there is perhaps an essential problem. In this case you are asked to contact the support (see paragraph 11.1).

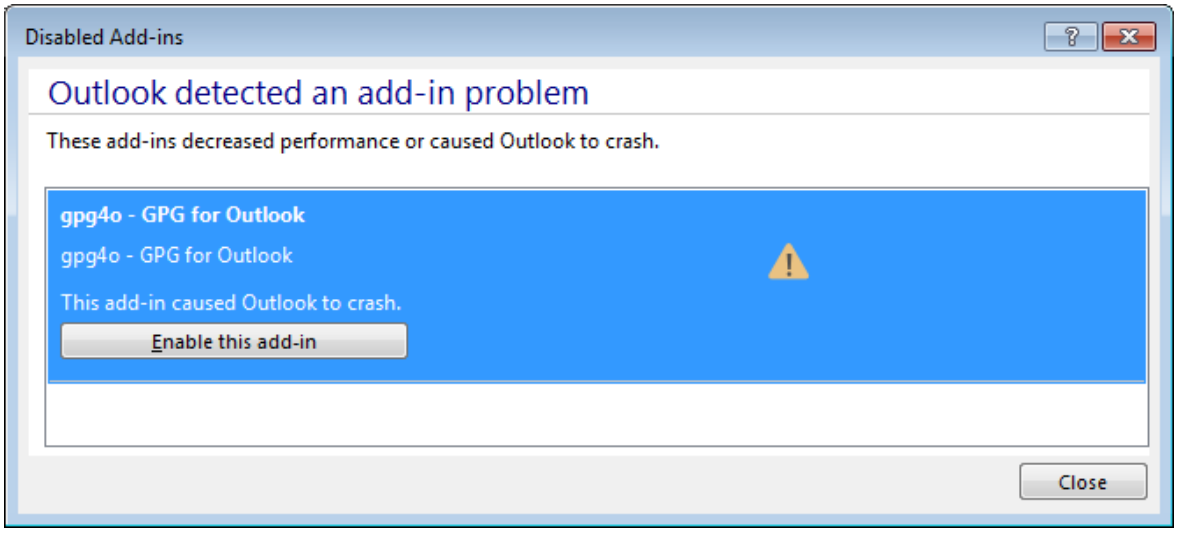


10.2.3 Microsoft Outlook 2013® and Outlook 2016®

Outlook 2013® and Outlook 2016® analyze the load times of add-ins and automatically disables add-ins with ordinarily longer uploading times.



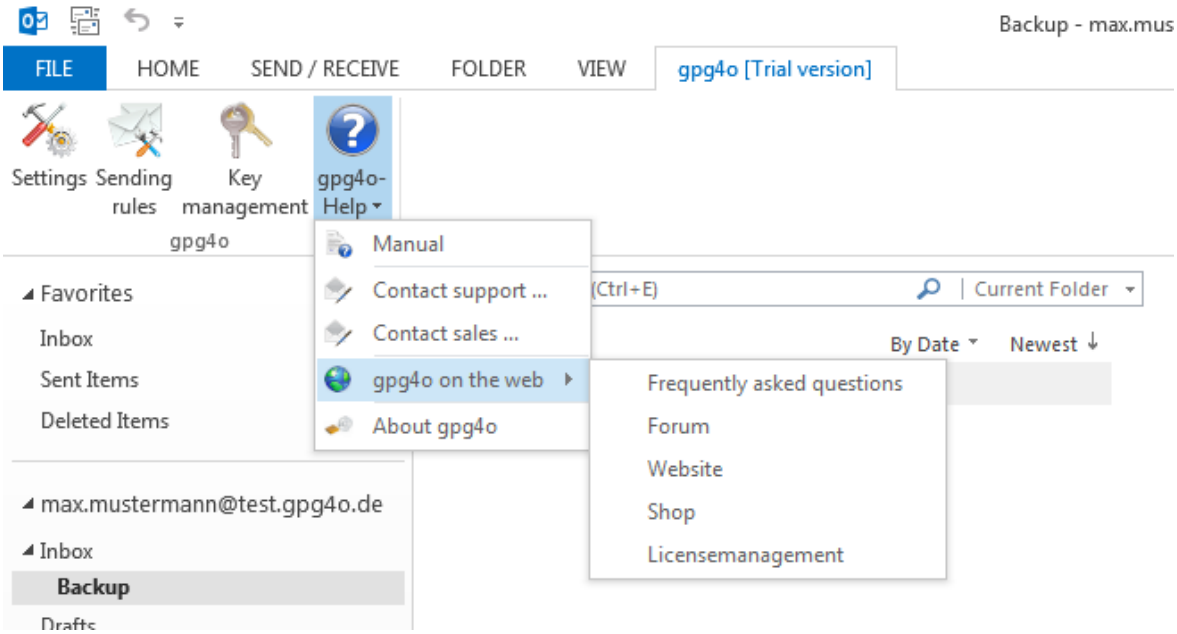
If this is true for you please go to **„File“** in the menu ribbon and there to **„Manage Add-Ins“**.



Select **gpg4o** and press the button **„Enable this add-in“**. Afterwards, please click the button **„Close“**.

11 Help Center

Via the help center you will get a simple and quick access to all important information regarding the utilization of **gpg4o**.



Here, you can open the manual, write an email to the technical support or to the sales department or inform yourself about **gpg4o** on the Internet.

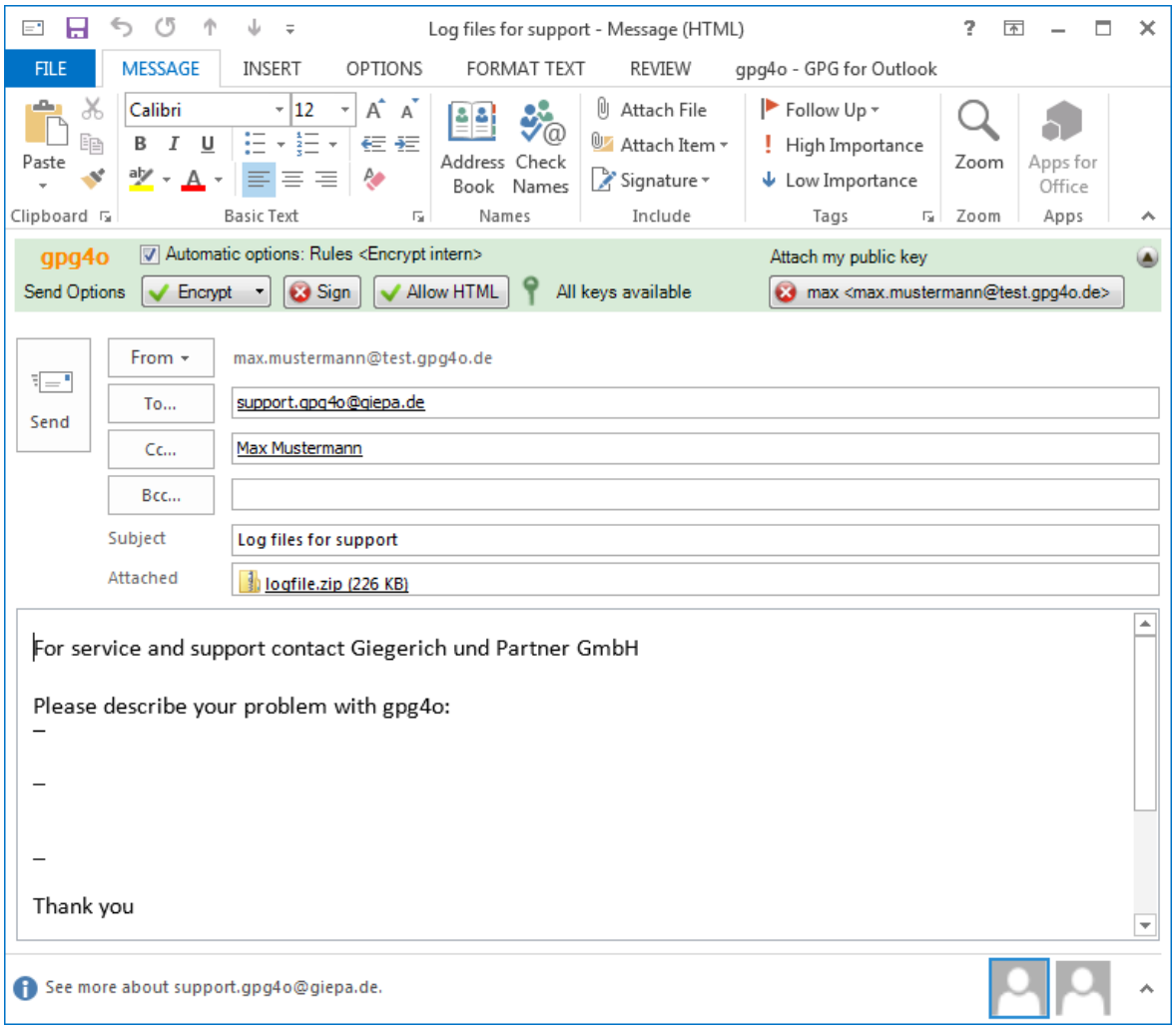
Via the menu entry **„gpg4o on the Web“** you will gain access to the following Web pages:

- Frequently asked questions
- Forum
- Website
- Shop
- Licensemanagement

In addition, you can call up the **„About gpg4o“** dialog where the installed version of **gpg4o** and information with regard to your license will be displayed to you. In this dialogue there is also the possibility of importing a license file. (see paragraph 4.3.1)

11.1 Sending Log-Files

In order to send the log files to our support, kindly click **„gpg4o – GPG for Outlook“** in the menu ribbon of Microsoft Outlook® . Here, select the push button **„Help Center“** and click the entry **„Contact support...“** then. Then, a preconfigured email will open automatically with the log files as attachment.



You are kindly asked to give precise description of the error occurred and of the steps which you have carried out shortly before said error showed. In so doing, you help us localize the error source and offer you a solution as fast as possible.

11.2 Contents of Log-Files

In order to optimize the efficiency of our development in the elimination of possibly occurring errors, status reports are written into so-called log-files by **gpg4o**. These status reports contain neither personal information nor passwords or contents of emails. Before sending the email together with the log-files you can see the information passed on by unpacking the attached zip-file. All files contained therein consist of plain text.

12 Uninstalling

If you uninstall **gpg4o** or also **GnuPG**, all generated and imported keys will remain and will be at your disposal again after a new installation.

12.1 Delete personal Data

If you want to delete your keys completely you should do this via the key management and uninstall the program **gpg4o** only then.

Alternatively, you delete the directory of **GnuPG**. In this directory you will find all personal data which are managed by **GnuPG** (Keyrings, trust settings and program configurations).

In addition, you should also delete the **gpg4o** user directory and the Microsoft Outlook® configuration directory. In these directories you can find the personal settings of **gpg4o**.

12.1.1 GnuPG Directory

`%AppData%\Roaming\gnupg`

Attention: Please mind that not only the program **gpg4o** accesses **GnuPG**-keys. Deleting the data may influence other programs.
By deleting the key data you will permanently lose access to your encrypted emails! Without the matching keys your emails cannot be decrypted.

12.1.2 gpg4o User Directory

`%AppData%\Roaming\Giegerich & Partner GmbH\gpg4o\`

12.1.3 Microsoft Outlook® Configuration Directory

`%AppData%\Local\Microsoft_Corporation\gpg4o.vsto_...`

This path varies depending on the computer and may be existent several times in similar form.

12.2 Uninstalling under Windows Vista, 7, 8 or 10

In order to uninstall **gpg4o** click **„Control Panel“** in the Windows start menu and browse to the item **„Programs“** there and afterwards to **„Uninstall a Program“**. You will now see the list of all programs installed on your computer. Select **„gpg4o – GPG for Outlook“** and click **„Uninstall“** in the menu.

12.3 Uninstalling GnuPG

In order to uninstall **GnuPG** click **„Control Panel“** in the Windows start menu and browse to the item **„Programs“** there and subsequently to the item **„Uninstall a Program“**. You will now see a list of all programs installed on your computer. Select the installed **GnuPG**

and click **„Uninstall“** in the menu.

13 Contact & Information

The IT-solution provider Giegerich & Partner GmbH based in Dreieich near Frankfurt on the Main specializes in the smooth and safe operation of networks and computer-controlled applications. In addition to consulting and conception the company undertakes the entire execution of IT projects as well as the operation of IT-systems and IT-solutions as outsourcing. Customer-specific individual solutions and the adaptation of IT-standard products to the requirements of companies belong to the strength of the IT-specialist.

From consulting to conception, realization and support –

Giegerich & Partner offers it all.

Further information can be found under: http://www.giepa.de/